Reference Guide

WinRoute Pro 4.1 BR

Para a configuração 22 da versão 4,1 e mais atrasado

Tiny Software Inc.

Índice analítico

Preparação e execução — Capítulo 2

Exemplos de implantação — Capítulo 3

Configuração do Firewall — Capítulo 4

LEIA ISTO PRIMEIRO

Caro cliente,

Obrigado por adquirir/avaliar o WinRoute Pro. A Tiny Software, empresa líder em tecnologia de firewall para redes de pequeno/médio porte, empreendeu um grande esforço e investimento em pesquisa para levar a você um roteador/firewall poderoso, porém fácil de usar, para uso com os sistemas operacionais Windows.

O WinRoute Pro é uma aplicação de rede que, juntamente com um PC, vem a ser um poderoso substituto de roteadores e firewalls baseados em hardware e muito mais caros. Como tal, necessita que a rede esteja instalada e configurada adequadamente. Portanto, é necessária certa experiência com um ambiente de rede.

Observe que (com base em nossas estatísticas) cerca de 90% dos problemas que os clientes têm ao conectar sua rede à Internet são devidos à uma configuração inadequada da rede. Este manual inclui diversos exemplos de configuração de rede, sendo que cada instalação pode ser diferente com diversas particularidades.

Recomendamos expressamente que esta documentação seja lida na sua íntegra e com muito cuidado. Ela foi preparada dentro da premissa que os seus usuários já possuem um conhecimento básico de redes assim como a habilidade e experiência para instalar uma rede local (Local Area Network - LAN).

Se mais adiante forem necessárias quaisquer dicas, check-lists e atualizações recentes, a Tiny Software orienta que seus clientes procurem inicialmente tais informações em sua seção de suporte online antes de fazer contato com o suporte técnico.

Gostaríamos de agradecer mais uma vez por adquirir/avaliar o WinRoute.

Obrigado,

TINY SOFTWARE, INC.

CAPÍTULO 1

DESCRIÇÃO DO WINROUTE

Neste capítulo

Resumo do WinRoute

O WinRoute Pro é o mais moderno software de **Roteador - Firewall para a Internet** tornando virtualmente sem esforço a tarefa de configurar todos os computadores em sua rede para compartilhar uma única conexão com a Internet! Conecte-se através de uma linha discada, DSL, Cabo, ISDN, LAN, T1, Rádio, DirecPC. Simples assim!

Administração remota

O WinRoute Administrator cuida da configuração e dos ajustes no WinRoute Engine. O WinRoute Administrator é uma aplicação individual (wradmin.exe) que pode ser executada em qualquer computador que tenha uma conexão ao computador do WinRoute Engine. O acesso ao Engine é assegurado por forte criptografia e uma senha.

Registro

O WinRoute Pro fornece um administrador com o mais moderno controle sobre o fluxo do tráfego através do computador host no qual está sendo executado. O Administrator pode beneficiar-se da análise do fluxo de pacotes ARP, TCP, UDP, ICMP, solicitações do DNS, informações de driver e muito mais. Todas as operações têm um carimbo de data/hora.

Roteador IP NAT

WinRoute inclui a (melhor) implementação da tecnologia Network Address Translation (NAT) disponível atualmente. É projetada para fornecer aos usuários o que há de mais moderno em capacidade de roteamento e proteção de rede. O driver NAT escrito exclusivamente para o WinRoute oferece uma solução de segurança de custo substancialmente inferior e comparável a produtos mais caros.

Roteamento NAT avançado

O NAT avançado permite que se modifique o endereço IP de origem em pacotes de saída com base em diversos critérios. Isto garante fácil integração de LANs atrás do WinRoute dentro do ambiente da WAN corporativa com diferentes segmentos, zonas desmilitarizadas (DMZs), redes privativas virtuais (VPNs), etc.

Servidores de hospedagem atrás do WinRoute

Por default, o WinRoute fecha todas as portas visando segurança máxima. Então, todas as solicitações não iniciadas são negadas, a menos que um mapeamento seja criado. A tecnologia Port Mapping (mapeamento de portas) permite que os usuários decidam como eles querem desviar pacotes IP que passem por qualquer interface operada pelo WinRoute. Com o WinRoute, os usuários podem definir que pacotes que estejam vindo para uma porta específica sejam passados para um determinado computador interno. Isto permite que eles ativem de forma segura um servidor da Web, servidor de correio, servidor de FTP, servidor VPN ou virtualmente qualquer outro tipo de servidor por trás do firewall.

Segurança do firewall

O WinRoute fornece aos usuários uma nível comparável de capacidade de firewall encontrada em soluções muito mais caras através de uma combinação de sua arquitetura NAT e sua habilidade para operar em um baixo nível. Isto permite ao WinRoute capturar tanto os pacotes de entrada como os de saída, que o faz inquebrável. O anti-spoofing é um complemento ao filtro de pacotes do WinRoute, para proteção adicional da rede contra ataques nos quais o invasor falsifica um endereço IP de origem.

Configuração simples de rede

O servidor DHCP e o forwarder DNS incluídos no WinRoute Pro simplificam a administração da configuração da rede. Os dois componentes são tecnologias maduras. O servidor DHCP do WinRoute pode facilmente substituir o servidor DHCP incluído no WindowsNT.

Servidor de correio

O servidor de correio do WinRoute, completo com compatibilidade com SMTP/POP3, virtualmente ilimitado em oportunidades de aliasing e classificação automática de correio, é extremamente versátil. Os usuários podem ter um ou mais endereços de correio eletrônico e trabalhar efetivamente em grupos (isto é, vendas, suporte, etc.) e cada grupo pode ser associado a mais usuários. Todos estes recursos estão disponíveis independentemente do tipo de conexão à Internet em uso.

Cache HTTP

A arquitetura do WinRoute inclui um mecanismo de cache inovador. Diferente dos servidores proxy com funcionalidade de armazenamento em cache, o cache do WinRoute armazena dados transitórios em um arquivo de tamanho predefinido ao invés de usar um único arquivo para cada objeto. Isto economiza de forma significativa o espaço em disco ocupado pelo cache, especialmente em ambientes (maioria dos Windows95) com FAT16.

Suporte abrangente a protocolos

WinRoute suporta todos os protocolos padrão da Internet incluindo:

IPSEC, H.323, NetMeeting, Net2Phone, WebPhone, UnixTalk, RealAudio, RealVideo, ICA, Winframe, IRC, FTP, HTTP, Telnet, PPTP, Traceroute, Ping, Year 2000 Aol, chargen, cuseeme, daytime, discard, dns, echo, finger, gopher, https, imap3, imap4, ipr, IPX overIP, netstat, nntp, ntp, ping, pop3, radius, wais, rcp, rlogin, rsh, smtp, snmp, ssl, ssh, systat, tacacs, uucpover IP, whois, xtacacs

Roteador com NAT

Nesta seção

Introdução ao NAT

NAT - Network Address Translation

Network Address Translation, ou NAT, é um dos recursos de segurança mais poderosos do WinRoute. NAT é um protocolo padrão da Internet usado para "esconder" endereços de redes privativas atrás de um único ou de múltiplos endereços. Uma versão do NAT chamada "IP Masquerading" tem sido popular por muitos anos junto à comunidade Linux e o WinRoute é um dos poucos produtos para a plataforma Windows que fornece realmente uma funcionalidade NAT entry-level.

O protocolo NAT pode ser implementado de diversas maneiras, mas essencialmente ele cria um espaço de endereços privativos praticamente ilimitado para redes internas que é "traduzido" pelo WinRoute de forma que a comunicação possa trafegar de e para redes públicas sem revelar informações restritas de sistemas internos. Sem ter conhecimento do espaço de endereços privativos na interface interna de um firewall do WinRoute, é praticamente impossível de atacar diretamente um sistema que esteja na rede interna protegida pelo NAT.

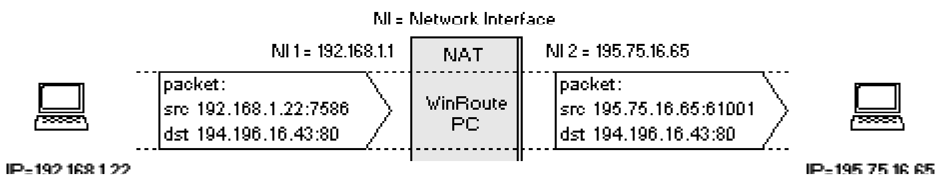
Como o NAT funciona

Network Address Translation (NAT) é um processo que modifica pacotes enviados de/para a rede local para/da Internet ou outras redes baseadas em IP.

No caminho de saída

Os pacotes de passagem pelo mecanismo de tradução de endereços **originados** na LAN são modificados ou traduzidos para se parecerem como se tivessem vindo do computador executando o NAT (este computador está conectado diretamente à Internet). O que realmente acontece é que o endereço IP de "origem" tem seu cabeçalho e substituído pelo endereço IP (público) do computador "NAT".

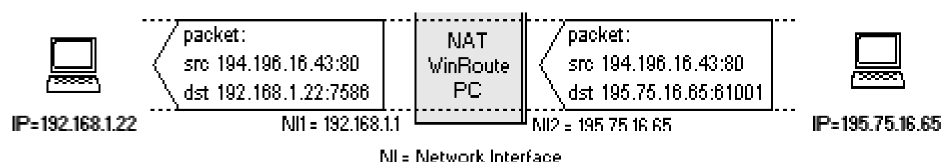
O mecanismo do NAT também cria uma tabela de registro de informações de cada pacote que passou para a Internet.



No caminho de volta

Os pacotes de passagem pelo NAT em direção **PARA** a LAN são comparados com os registros mantidos pelo mecanismo do NAT. Lá o endereço IP de "destino" é modificado (com base nos registros do banco de dados) para o endereço IP interno de classe privativa de forma a encontrar o computador na LAN .

Lembre-se que o pacote veio com o endereço IP público do computador NAT originalmente como um "destino". O mecanismo do NAT teve que modificar esta informação de forma a enviar o pacote para o destinatário correto dentro da rede local.



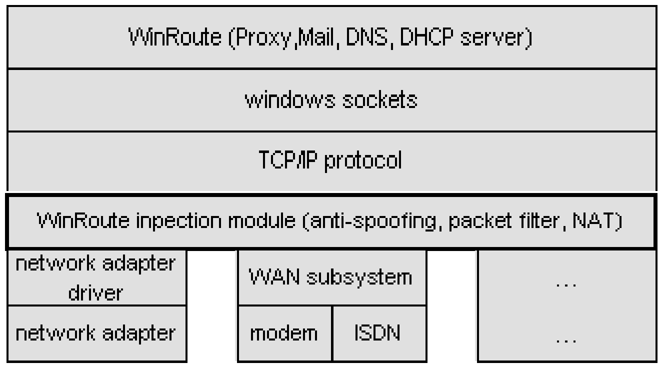
Arquitetura do WinRoute

Arquitetura do WinRoute

Para uma interligação de rede avançada, é muito útil entender como o WinRoute funciona. A partir das explanações e dos exemplos listados abaixo, o WinRoute demonstra que é uma excelente solução para quase qualquer configuração de rede.

1. **Segurança total**
   O WinRoute funciona **abaixo da pilha TCP** no nível IPSEC. Em outras palavras - ele captura os pacotes de **saída** e de **entrada ANTES** que tenham a chance de entrar no computador.

Esta concepção avançada faz da segurança do WinRoute quase **inquebrável**



2. **Suporte total a protocolo**
   O WinRoute é um ROTEADOR baseado em software. Como tal, diferentemente dos servidores Proxy como WinGate ou WinProxy, o WinRoute pode permitir a passagem de quase qualquer protocolo da Internet. Ao mesmo tempo o WinRoute verifica cada pacote com a utilização da segurança avançada e dos recursos do firewall inerentes ao projeto do software. Em sistemas executando o Windows 95 e 98, o WinRoute manipula o roteamento dos pacotes. Em sistemas executando o Windows NT, o sistema operacional do NT executa o roteamento e o WinRoute gerencia a funcionalidade do NAT e outros dados.

3. **Total flexibilidade**
   O WinRoute executa o NAT (Network Address Translation) nas interfaces de sua escolha. O WinRoute também cumprir quaisquer regras de segurança definidas previamente nas interfaces específicas. Isto dá ao usuário uma grande liberdade quando da preparação e da configuração das opções de segurança.

Configurando o NAT nas duas interfaces

Você pode querer usar o WinRoute apenas como o **roteador de acesso neutro (neutral access router)** para o tráfego (de pacotes) dirigido da **Internet** para a **rede local**. No caso de você já possuir uma solução de acesso compartilhado à Internet; se esta solução não permitir que você ative servidores e aplicações na sua rede privativa e que precisam estar acessíveis pela Internet, então o WinRoute pode ser a solução certa nesta configuração muito específica.

Os serviços que podem estar acessíveis pela Internet são:

- servidor telnet (p. ex. AS400)
- servidor WWW
- servidor de correio
- PC Anywhere
- servidor de FTP
- … e qualquer outro servidor (serviço) ao qual se possa ter acesso em uma determinada porta.

O WinRoute proverá os seus usuários/clientes com acesso confiável e seguro a tais serviços. A configuração do WinRoute para estes serviços está descrita em outros capítulos. Você deverá realizar os seguintes ajustes diferentemente:

Recurso	Recomendação original	Neste caso
NAT na interface com a Internet	ON	ON
NAT na interface interna (LAN)	OFF	ON
O endereço IP da interface interna do WinRoute como o gateway padrão para os outros computadores dentro da rede	SIM (uma NECESSIDADE)	NÃO (desnecessário)

Em outras palavras - usar o WinRoute permitirá que você disponibilize o acesso pela Internet a determinados serviços SEM a necessidade de alterar a configuração da rede.

➢ ***Observe! Configurar o NAT em ambas as interfaces NÃO permitirá que você use o WinRoute para compartilhamento de acesso à Internet!***

Os ajustes do gateway padrão neste exemplo dão a você grande liberdade. Você pode manter todos os seus ambientes existentes inalterados. Para manter os roteadores e as rotas estabelecidas na operação da sua rede, ao adicionar novos computadores executando o WinRoute você pode permitir que usuários externos tenham acesso aos servidores dentro de sua rede local.

Isto é importante (por exemplo) quando você tem uma WAN e quer permitir o acesso de usuários externos ao seu AS400 (servidor de telnet) ou à sua rede interna através de PPTP.

Para isso você deve seguir os seguintes passos:

1. Ligue um computador com duas interfaces à sua rede. Uma interface (externa) será ligada à Internet enquanto a outra (interna) se ligará à sua rede existente.
2. Designe a interface externa com o endereço IP que será usado para o acesso aos serviços/servidores que você deseja que estejam disponíveis para acesso pela Internet.

3 Designe o endereço IP interno manualmente ou através do servidor de DHCP

4 Ajuste o WinRoute para executar o NAT nas duas interfaces

5 Ajuste o mapeamento de porta para os serviços que você deseja que sejam executados dentro de sua rede

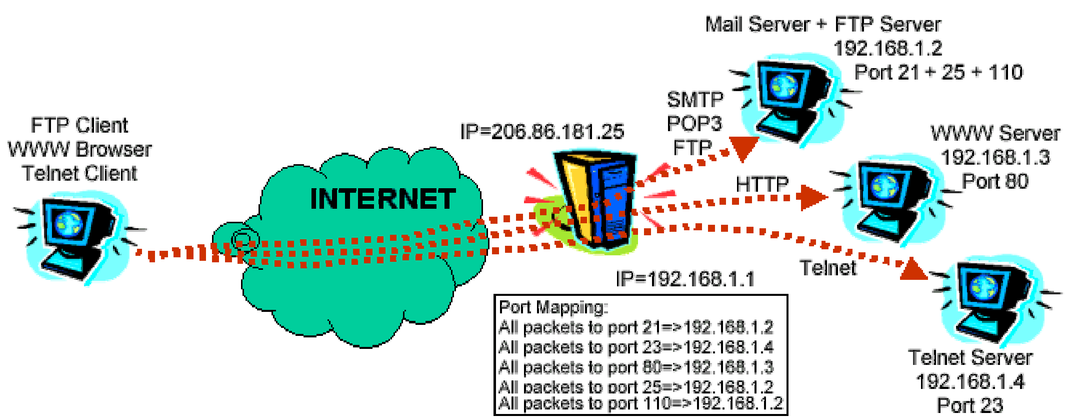
Após estes ajustes os usuários externos estarão aptos a ter acesso aos seus serviços internos (em execução em portas específicas) a partir da Internet. A segurança de tal acesso é garantida pelo firewall do WinRoute.

Mapeamento de porta - encaminhamento de pacote

O WinRoute executa o NAT, que torna a rede protegida inacessível por acessos externos. Usando mapeamento de portas (ou Port Address Translation - PAT) os serviços públicos como um servidor WWW ou um servidor de FTP, além de outros em execução na sua rede privativa, podem estar acessíveis pela Internet.

Como o mapeamento de porta funciona

Cada pacote recebido de uma rede externa (da Internet) tem seu atributos (quer dizer o protocolo, a porta de destino e o endereço IP de destino) verificados quanto à sua compatibilidade com uma entrada na tabela de mapeamento de portas (Protocolo, Listen Port, Listen IP). Se o pacote de chegada atende aos critérios desejados, é modificado e enviado para o endereço IP da rede protegida definido como o "IP de destino" na entrada da tabela e a porta definida como "Porta de Destino".



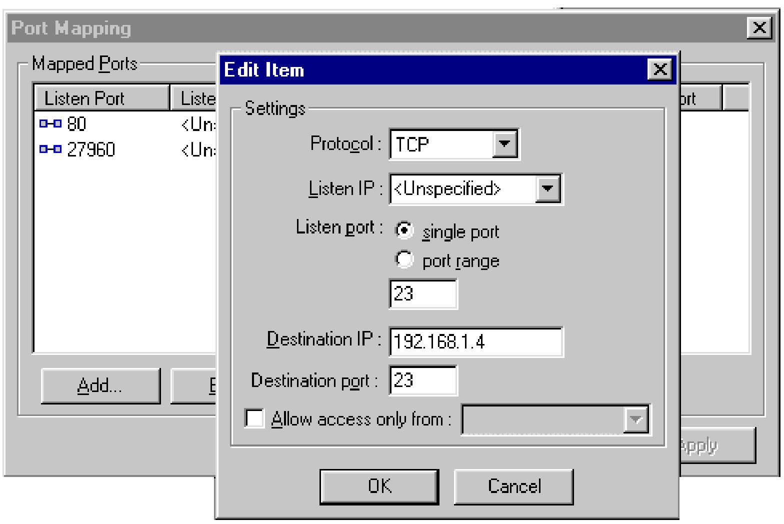
Por exemplo, se você tem um servidor da Web executando no IP interno 192.168.1.3 e deseja permitir o acesso de usuários da Internet ao mesmo. Haverão solicitações dos usuários da Internet chegando ao seu computador do WinRoute com endereço IP externo igual ao registro DNS do seu servidor da Web www.seudomínio.com. Como todas as solicitações ao servidor da Web chegam na porta 80 você irá configurar o mapeamento de porta informando que toda a comunicação TCP na porta 80 será desviada para o endereço IP interno 192.168.1.3.

Configuração do mapeamento de porta

Para definir o mapeamento de porta

1 Vá ao menu *Configurações->Avançadas->Mapeamento de porta*

2 Adicione um novo mapeamento de porta:



Protocolo

Selecione o protocolo usado pela aplicação/serviço. Algumas aplicações/serviços usam os protocolos TCP e UDP ao mesmo tempo. Por exemplo, o módulo WinRoute Administrator

IP de escuta (Listen IP)

O endereço IP para o qual os pacotes de entrada estão se dirigindo. Normalmente este é o endereço IP associado com a sua interface com a Internet. Observação: você deve ter mais de um endereço IP associado com a interface (se você tiver mais servidores da Web, etc.)

Porta de escuta (Listen Port)

O número da porta para a qual os pacotes estão indo.

IP de destino

O endereço IP dentro de sua rede local no qual está sendo executado o servidor (serviço) que atende aos pacotes de chegada (servidor da Web, servidor de FTP, etc.)

Porta de destino

A porta na qual a aplicação de destino está "escutando". Tipicamente o mesmo número da porta de escuta

Permitir acesso apenas de

Você pode especificar o endereço IP do qual deseja permitir o acesso. Isto é muito importante para aumentar a segurança, no caso de você definir o mapeamento de porta para aplicações de administração remota tais como o WinRoute administrator, PC Anywhere, etc. Você pode especificar o grupo de endereços IP. Inicialmente você deve criar tal grupo na caixa de diálogo "Grupos de endereços".

Mapeamento de porta para sistemas multi-homed (mais endereços IP)

Você pode ter mais endereços IP atribuídos à interface com a Internet e executar diversos serviços dentro de sua rede aos quais você deseja que se tenha acesso pela Internet.

Exemplo com 5 servidores WWW

Como um exemplo considere que você deseja ativar 5 servidores da Web onde cada um deles tem um domínio distinto associado a um endereço IP diferente.

Em um quadro como este você atribuirá 5 endereços IP à sua interface externa (ligada à Internet) e ativará servidores da Web em outros computadores dentro de sua rede interna.

Cada servidor da Web pode executar em um computador diferente ou você pode atribuir mais endereços IP a um computador em sua rede interna e executar todos os servidores da Web no mesmo (computador).

A seguir você definirá 5 mapeamentos de portas em uma caixa de diálogo de Mapeamento de porta. Para cada servidor da Web (domínio) você definirá:

- Endereço IP de escuta (endereço IP público associado ao domínio).
- Porta de escuta: 80 em nosso exemplo
- Endereço IP de destino: o endereço IP onde é executado o servidor da Web
- Porta de destino: 80 (para www)

Para mais exemplos sobre Mapeamento de porta avançado consulte o capítulo Redes (Interligação de) mais avançadas.

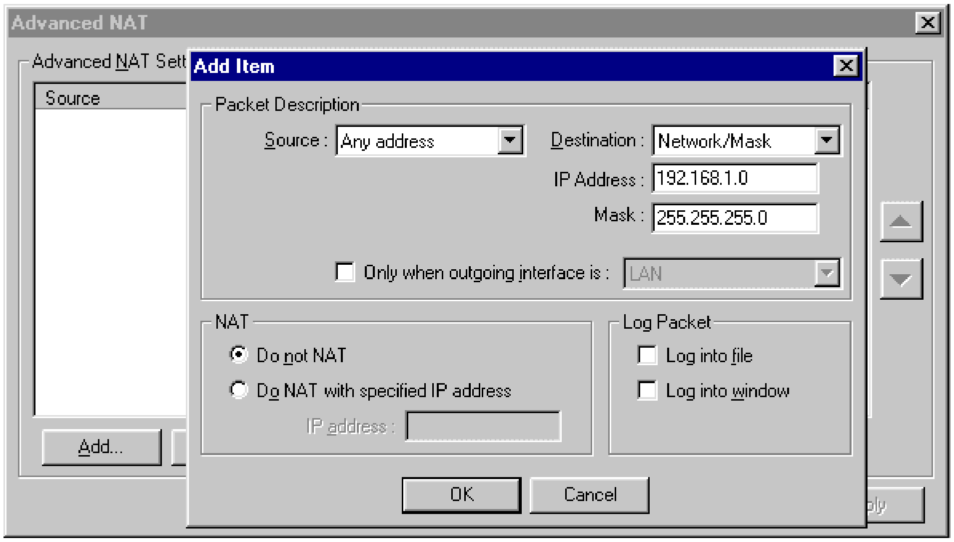
Multi NAT

O WinRoute permite configurações simples do **NAT** (Network Address Translation) bem como as mais complicadas. Você pode especificar, com base no endereço IP de **origem** ou **destino** do pacote, que o NAT pode ser fornecido com algum **outro endereço IP** (isto é, os pacotes poderiam parecer como oriundos de outro endereço IP) ou que o **NAT** não será executado de nenhuma maneira.

Tais configurações são de grande importância, em ambientes de redes mais complexos onde:

- certos computadores poderiam apresentar **outro** endereço IP que não o principal usado pelo **resto** da rede
- você tem filiais conectadas à **WAN** com espaço de endereço privativo e deseja compartilhar **um** acesso à Internet com todas elas
- você tem diversos segmentos por trás do WinRoute onde um segmento (adicional) é uma zona desmilitarizada (DMZ) com endereços IP públicos
- você deseja ter endereços IP públicos dentro de seu rede privativa (Lembre-se! Você precisa confirmar com o seu provedor de acesso que estes endereços IP serão roteados através de seu endereço IP principal.)

Você pode encontrar alguns exemplos do uso de "Configurações avançadas do NAT" no capítulo Redes (Interligação de) mais avançadas.



Endereço IP de origem, endereço IP de destino

Você pode efetuar configurações avançadas do NAT com base no endereço IP do qual os pacotes são enviados (origem) ou para onde são remetidos (destino). Como uma origem você inserir o IP do Host, a rede inteira (limitada pela máscara da rede) ou o grupo de endereços IP criado anteriormente no menu Configurações->Avançadas->Grupos de endereços.

Não usar NAT

Se selecionado, os pacotes de passagem pela interface com a Internet não serão alterados

Usar NAT com o endereço IP especificado

Se selecionado, os pacotes de passagem pela interface com a Internet serão alterados para como se fossem originados de um endereço IP desejado.

Tabela de interface

A tabela de interface é uma caixa de diálogo na qual o WinRoute exibe todas as interfaces disponíveis no computador que ele pode reconhecer. Se você tiver mais interfaces que as exibidas pelo WinRoute é provável que o driver de tal(is) interface(s) não tenha(m) sido carregado(s) de forma apropriada pelo sistema operacional e o WinRoute não o(s) possa ler.

Você pode ver:

Nome da interface

você pode alterar o nome ao selecionar “propriedades” e alterá-lo.

Endereço IP

o valor definido nas propriedades do TCP/IP da interface. Se estiver definido que a interface deve pegar o endereço IP do servidor DHCP você pode ver o endereço IP atual atribuído à interface.

NAT “On” ou “Off”

Se estiver definido que o NAT deve ser executado na interface, então “On” é exibido nesta coluna

Suporte a VPN

Como mencionado anteriormente, o WinRoute é inteiramente apto para o tráfego de passagem dos dois mais populares protocolos de VPN em uso hoje em dia: o IP Security protocol (IPSec) proposto pelo IETF, e o Point-to-Point Tunneling protocol (PPTP), tornado popular nos últimos anos devido à sua inclusão com o sistema operacional cliente Microsoft Windows.

Firewall com filtragem de pacote

Nesta seção

Visão geral da filtragem de pacote

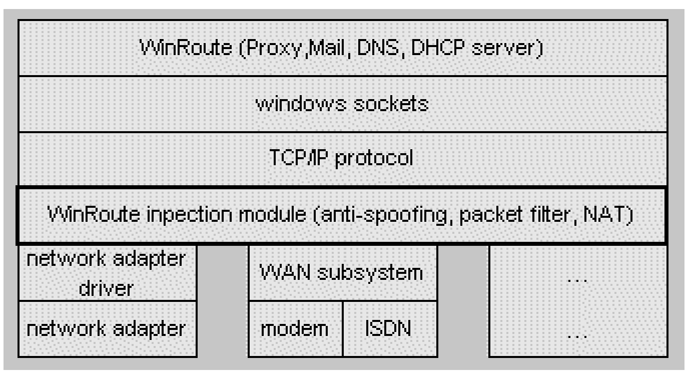
O coração de qualquer mecanismo de controle de acesso de um firewall é, evidentemente, a tecnologia pela qual ele concede ou nega autorização a pacotes destinados a redes protegidas. O WinRoute implementa uma das tecnologias mais comumente usadas para controle de acesso a rede: filtragem de pacotes. Ainda que o WinRoute implemente outros mecanismos de controle de acesso, tais como um servidor proxy integrado com cache para os protocolos HTTP, FTP e Gopher, o objetivo primeiro deste recurso é que seja um elemento de melhoria no desempenho de saída e não um recurso de segurança.

A filtragem de pacote tem uma longa tradição na comunidade de segurança e ainda é amplamente implementada em produtos como o sistema operacional de dispositivo de rede IOS da Cisco. Configurados de forma adequada, os filtros de pacote podem se tornar bastante seguros e são particularmente apropriados para sites da Internet com alto volume na medida em que fornecem os benefícios do melhor desempenho.

Arquitetura

Os firewalls são tipicamente construídos sobre plataformas rígidas e o software em si normalmente é difícil de ser contornado. Contudo, uma grande fraqueza em muitos dispositivos de segurança de rede ocorre durante a pequena janela de tempo entre o momento em que o hardware está ativamente capaz de rotear o tráfego e o software assume o controle das interfaces de rede. Desde este momento crítico, a segurança pode estar completamente comprometida.

O driver do WinRoute, ou Engine, se ativa ao mesmo tempo em os arquivos do núcleo do sistema operacional Windows (o kernel) são carregados para a memória; especificamente, o mecanismo (Engine) é carregado antes dos módulos NDIS (Network Device Interface Specification), de forma que nenhuma conectividade da rede seja suportada antes que o WinRoute esteja ativo. Portanto, a proteção de todas as interfaces está ativa antes que qualquer tráfego mal intencionado ou outros ataques possam ser armados contra o sistema. Isto mostra-se mais favorável em comparação com produtos isolados do tipo de detecção de intrusão que são executados como um serviço e não estão ativos até que o sistema tenha terminado o processo de boot.



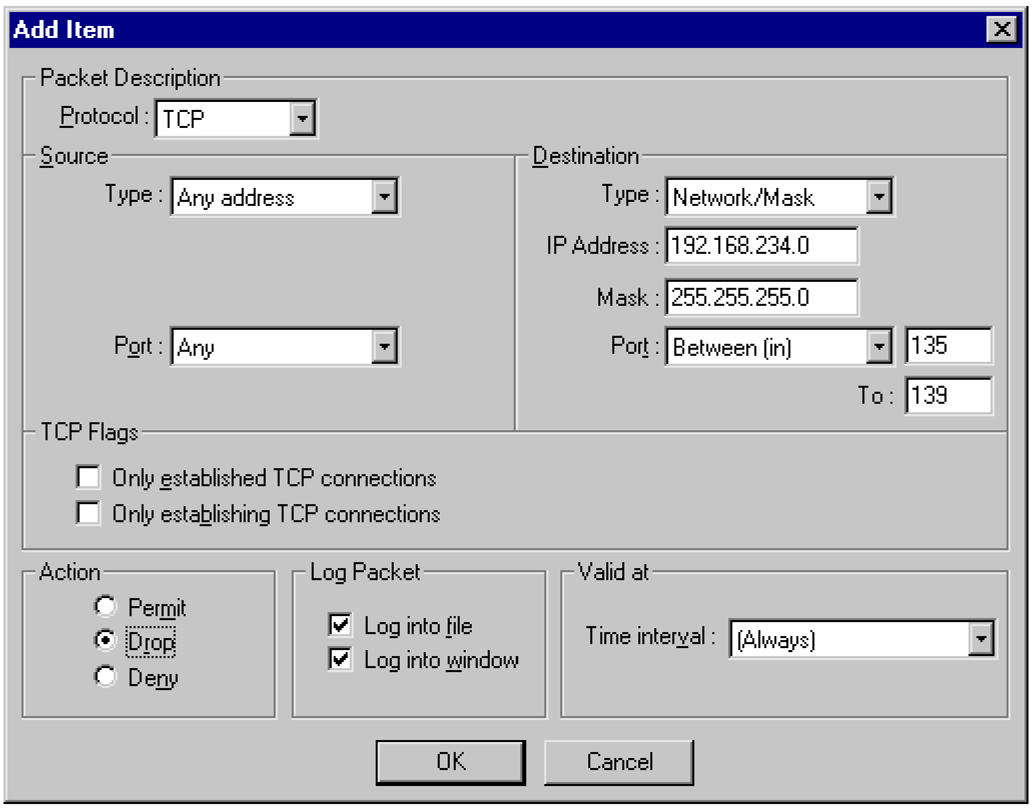
O WinRoute "empacota" o NDIS em um padrão proprietário de forma que todo o tráfego TCP/IP é desviado do driver da placa de rede (NIC) para o Engine antes de prosseguir para a pilha de comunicação de rede do próprio sistema operacional.

Esta inserção de baixo nível no sistema operacional permite ao WinRoute Engine uma perspectiva única sobre todo o tráfego de rede que chega a qualquer interface (seja de entrada ou de saída). Assim como ocorre com muitos produtos de firewall de categoria empresarial tais como o Firewall-1 da Check Point, o WinRoute tem a condição de fazer a primeira decisão de conceder ou negar autorização a um dado pacote. De novo, isto evita ataques mal intencionados contra outras frentes do sistema operacional ou outro software que poderia contornar a segurança oferecida por um firewall. Isto certamente é desejável para gateways para a Internet com interface externa, mas também pode fornecer grandes benefícios a hosts isolados com requisitos de alta segurança ou anonimato, como um sistema de detecção de intrusão. O software de detecção de intrusão como um Real Secure da Internet Security Systems (ISS) ficaria praticamente invisível em um host protegido pelo WinRoute.

Finalmente, o WinRoute Engine assume toda a funcionalidade de roteamento de comunicação do sistema operacional Windows básico (seja ele o Windows 9x, NT ou 2000). Isto assegura que, em caso da falha do WinRoute Engine por qualquer razão, nenhum tráfego será roteado entre as redes. Esta postura de "fechar em caso de falha" tem sido o padrão tradicional das configurações de firewall por muitos anos e serve para proteger redes privativas no case de falhas comuns do sistema.

Regras

A despeito das questões teóricas que envolvem a filtragem de pacotes, o ponto principal de falha dos sistemas de firewall de modem é o problema da configuração, especialmente a realizada por equipe de administração sem experiência. O WinRoute torna a configuração dos filtros uma tarefa simples e suficientemente flexível de forma que mesmo os administradores de rede novatos possam implementar uma configuração segura com um pouco de conhecimento de TCP/IP e uns poucos cliques com o mouse, como está ilustrado na tela capturada a seguir.



As regras do filtro podem ser aplicadas em uma base "por interface" para todas as entidades a seguir:

- um único endereço IP
- uma lista de endereços IP definidas pelo administrador
- uma rede ou sub-rede inteira

É importante observar também que os filtros podem ser definidos para o tráfego de entrada e de saída.

Estes recursos permitem o ajuste preciso das regras de acesso às exigências de segurança de quase qualquer organização. Por exemplo, um grupo de desenvolvedores para a Web poderia ter o acesso concedido a recursos externos específicos tais como staging servers (servidores de preparação ou pré-teste) de FTP anônimo, ou uma lista especificada de endereços internos poderia ser designada como acessível por redes de parceiros externos para a cópia ou retirada de arquivos eletrônicos. A configuração de entrada/saída permite a proteção contra ataques mal intencionados "às avessas" tais como o Back Orifice (BO) ou servlets de DDOS (distributed denial of service) que tentam se comunicar por protocolos não confiáveis e voltam através do firewall com ataques externos.

As regras podem Permitir, Derrubar ou Negar o tráfego especificado; a ação de "Derrubar" revela o mínimo de informação sobre o firewall para agressores em potencial, a medida que não envia uma resposta ICMP do filtro de acessos proibidos administrativamente ou de Reset/Acknowledge do TCP (o primeiro passo na seqüência padrão de envio e confirmação por três vias do TCP - three-way TCP handshake).

As regras podem ser priorizadas para agir em uma ordem específica, definida pelo usuário em pacotes de entrada e saída. O uso mais popular deste recurso é o de adicionar as assim chamadas "regras de limpeza" ("cleanup rules") para filtrar listas que bloqueiam todo o tráfego não especificamente autorizado por regras anteriores que têm maior prioridade na lista (para um exemplo de uma regra de limpeza, consulte as definições de Exemplo de regra básica de filtragem de pacote, mais adiante neste documento).

Protocolos

Os protocolos suportados pelos filtros de pacote do WinRoute incluem:

- raw IP
- sete tipos de ICMP (ou todos)
- TCP
- UDP
- PPTP.

A habilidade para permitir ou bloquear tipos de ICMP raw específicos ou protocolos raw IP é inestimável para os administradores de rede que estão de frente com uma lista sempre crescente de exigências de aplicações para suportar. Em particular, os relativamente novos protocolos VPN tais como o IPSec trafegam sobre protocolos raw IP 51 e 52, o que seria impossível de filtrar com o uso de alguns dos mais restritos produtos de firewall do mercado atual que são capazes apenas de controlar protocolos baseados em UDP ou TCP.

Anti-Spoofing

Além disso, o WinRoute fornece recursos anti-spoofing, o que evita pacotes com endereços de origem inválidos de serem criados dentro de uma rede. O anti-spoofing poderia ter evitado os ataques ICMP smurf relatados em fevereiro de 2000 com os ataques DDoS em sites importantes da Web como o Yahoo e Buy.com. Os usuários do WinRoute podem descansar confortavelmente sabendo que suas redes são fontes improváveis de tais ataques se eles implementam este recurso.

Análise de logs e pacotes

Nesta seção

Sobre os logs e a análise

Uma função crítica de qualquer produto de segurança é a habilidade de registrar eventos em todos os momentos de uma forma bem detalhada. O WinRoute registra seis diferentes logs do tráfego que atinge o firewall, incluindo pacotes que passam por ele, atividades de usuários, ações de filtragem e assim por diante. Uma descrição de cada log é mostrada na tabela a seguir:

Log de HTTP	Exibe apenas os dados HTTP de passagem pelo servidor proxy do WinRoute; inclui o endereço IP de origem e nome de usuário, data e hora e consultas e respostas do HTTP
Log de mensagens	Registra todas as operações do servidor de correio embutido no WinRoute; registra as atividades de envio/recebimento do SMTP e do POP3
Log de segurança	Mostra todas as atividades definidas como "Registrar log em janela/arquivo" em regras de filtragem de pacotes (consulte abaixo a descrição detalhada dos itens registrados)
Log de discagem	Registra as informações do uso das interfaces de discagem (dial-up) monitoradas pelo WinRoute
Log de depuração	Configurações "a la carte" para registrar todos os pacotes ARP, ICMP, UDP, TCP e/ou DNS que passam fisicamente por qualquer interface do roteador do WinRoute; configuração precisa disponível através do menu Configurações | Avançadas | Informações de depuração, na guia Depuração.
Log de erros	Exibe todas as operações mal sucedidas que ocorrem em qualquer módulo do WinRoute em execução

O Log pode ser exibido no console do WinRoute Administrator, ou gravado em um arquivo, ou ambos. Os arquivos de log são armazenados no diretório \%installroot%\Logs, que é acessível apenas às contas NT/2000 dos administradores, operadores de servidor, do sistema (SYSTEM) e do criador proprietário (CREATOR OWNER) que instalou o WinRoute.

As informações de log registradas pelo Log de segurança do WinRoute são completas, incluindo todas as informações necessárias para iniciar uma investigação adequada dentro de atividades potencialmente mal intencionadas:

- Data
- Hora
- Regra de filtragem de pacote acionada
- Interface
- Ação (Permitir, Derrubar, Negar)
- Protocolo
- Endereço IP e porta TCP de origem
- Endereço IP e porta TCP de destino

O teste sob condições adversas de alto tráfego não afeta a capacidade de registro do log do WinRoute. Isto é crítico para prevenir a perda de valiosos dados judiciais assim como para moderar as situações potenciais de DDoS (denial-of-service) onde a funcionalidade do firewall é desligada se o sistema de registro do log é subjugado.

Log de depuração

O **Log de depuração** é o mais importante log no WinRoute. Ele permite que se veja **todos os pacotes IP** (TCP, UDP, ICMP, ARP, DNS) que passam fisicamente por quaisquer interfaces presentes no computador do WinRoute.

Na janela **Eventos de depuração** você pode ver o conjunto de eventos que desejar que seja exibido.

Como ler o log?

A partir da esquerda você pode ver o seguinte:

Data e hora - a data e a hora exatas em que o evento ocorreu ou que o pacote passou pela interface.

O protocolo - o tipo de protocolo do pacote

Nome da interface De/Para - o nome da interface e se o pacote foi **Para (to)** ou veio **De (from)** uma interface (imagine que o WinRoute está sendo executado no PC e as interfaces funcionam como "portas" entre o computador e a rede).

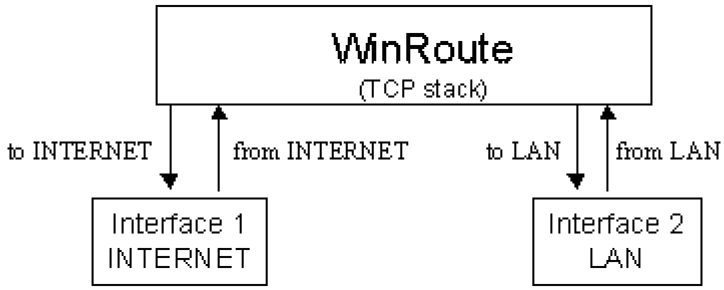
Endereço IP de origem -> Endereço IP de destino - os endereços IP de origem e destino presentes no pacote.

Os sinalizadores (flags) - informação adicional sobre a ação.

Exemplo:

```
[10/Nov/1999 09:32:38] TCP: packet 511464, from lan,
length 1514, 192.168.1.7:2442 -> 192.168.1.1:25,
flags: ACK

[10/Nov/1999 09:32:38] TCP: packet 511465, to lan,
length 54, 192.168.1.1:25 -> 192.168.1.7:2442, flags:
ACK
```


WinRoute
(TCP stack)
to INTERNET
from INTERNET
to LAN
from LAN
Interface 1
INTERNET
Interface 2
LAN

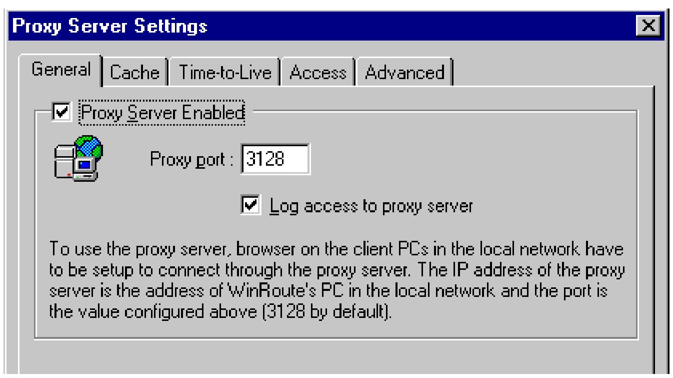
Log de HTTP (Proxy)

O log de HTTP (Proxy) é uma ferramenta poderosa que ajuda você a ficar de olho nas atividades dos usuários na Internet. Ele fornece informações de mais fácil utilização sobre usuários que têm acesso à Web do que as poderiam ser obtidas do log de depuração.

Quando o log funciona?

O log de HTTP (Proxy) apenas exibe dados que passam pelo servidor proxy do WinRoute. Isto significa que, se você quiser obter dados do servidor proxy você deve forçar seus usuários a usá-lo na conexão à Internet. Consulte os capítulos com exemplos de firewall ou de servidor proxy.

Além disso - você precisa habilitar o acesso do log à configuração do servidor proxy.



Como ler o log de HTTP (Proxy)?

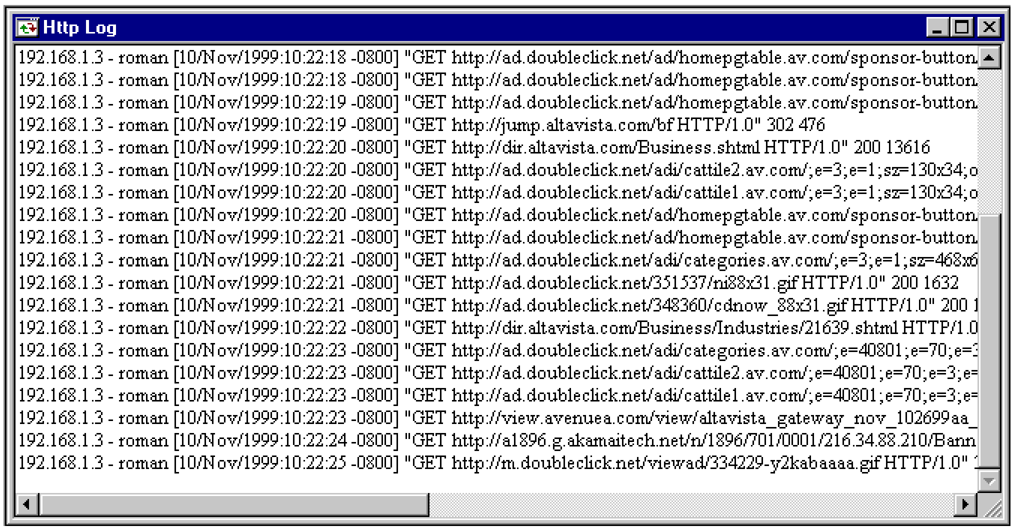
```
192.168.1.3 - roman [10/Nov/1999:10:22:20 -0800] "GET
http://dir.altavista.com/Business.shtml HTTP/1.0" 200
13616
```

Da esquerda para a direita:

Endereço IP - nome - o nome e o endereço IP atual do usuário que está fazendo acesso à Internet

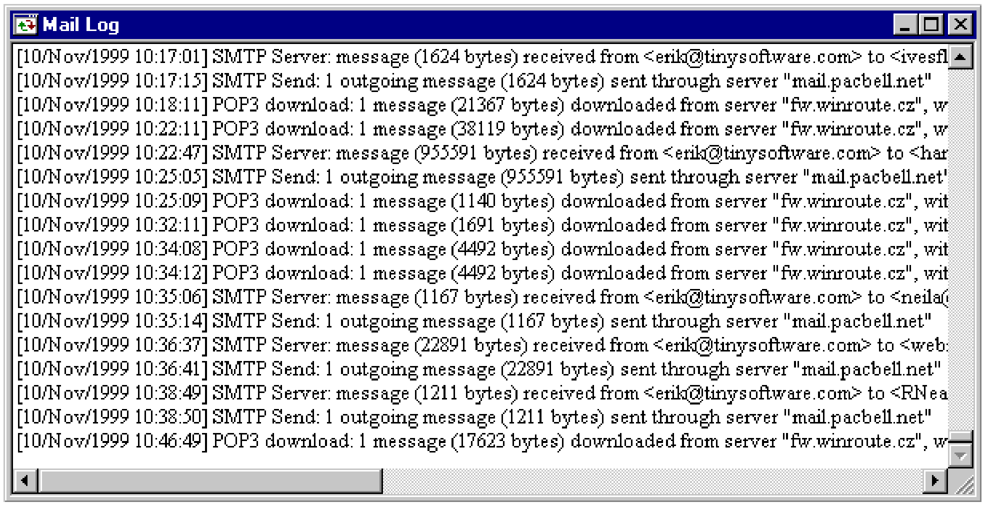
Data e hora - a data e a hora do acesso

GET "http..." - O alvo do acesso



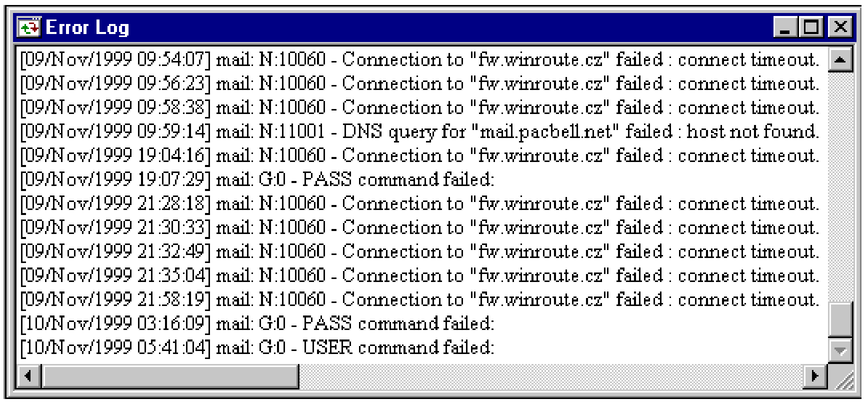
Log de mensagens

O log de mensagens registra todas as operações do servidor de correio embutido no WinRoute. Você pode ver quantas mensagens foram enviadas, recebidas, para onde as mensagens foram enviadas, etc. Todas as operações apresentam a data e a hora em que foram realizadas.



Log de erros

O log de erros exibe todas as operações mal sucedidas nos módulos do WinRoute que estão em atividade. Como resultado você pode ver os erros na troca de mensagens, no servidor DNS, etc.



Servidor DHCP

Nesta seção

Visão geral do DHCP

Em uma rede, cada computador precisa ter seu protocolo TCP/IP configurado apropriadamente. Isto significa que o endereço IP, a máscara de rede, o endereço do gateway default, o endereço do servidor DNS, etc. precisa ser configurado em cada computador. Se o responsável pela configuração tiver que ajustar os parâmetros manualmente em um grande número de estações, será difícil evitar erros, p.ex. usar o mesmo endereço duas vezes - o que pode provocar colisões e também, consequentemente, um funcionamento incorreto de toda a rede.

O protocolo DHCP (Dynamic Host Configuration Protocol) é uma implementação do WinRoute projetada para simplificar a tarefa de administração de uma rede. O DHCP é usado para uma configuração dinâmica do protocolo TCP/IP nos computadores. Durante o processo de boot, o computador com o cliente DHCP envia uma solicitação. Quando o servidor DHCP recebe a solicitação, escolhe parâmetros de configuração do TCP/IP para o cliente. Os parâmetros são o endereço IP, a máscara de rede, o gateway default, o endereço do servidor DNS, nome de domínio do cliente, etc. Usando esses parâmetros, o servidor prepara uma resposta e a envia para o cliente.

O servidor pode atribuir uma configuração para o cliente por um tempo limitado apenas (o assim chamado tempo de liberação - lease time). O servidor sempre atribui o endereço IP de forma que este não vá colidir com qualquer outro endereço atribuído pelo DHCP para um outro cliente.

Com um servidor DHCP disponível, basta habilitar a opção "Obter endereço IP do servidor DHCP" e o servidor DHCP assume a responsabilidade pela configuração apropriada do TCP/IP nas estações. Esta maneira pode ajudar a reduzir significativamente os custos de manutenção e gerenciamento da rede.

- ***Se alguns computadores em sua rede não são configurados dinamicamente pelo DHCP, mas ao invés disso usam uma configuração fixa, você precisa ter certeza de que os parâmetros usados pelo DHCP não irão colidir como s usados nas configurações fixas.***

Forwarder DNS

Nesta seção

Sobre o encaminhamento de DNS

Cada computador conectado à Internet é identificado por um único endereço IP numérico. Para se conectar a um computador na Internet, seu endereço precisa ser conhecido do computador que está fazendo a conexão. Uma vez que os endereços IP são difíceis de lembrar, o DNS (Domain Name Service) foi criado.

O DNS é um banco de dados de nomes descritivos que presumivelmente são fáceis de lembrar. Dessa forma o usuário não precisa conhecer o endereço IP do servidor com o qual ele/ela deseja se comunicar. Basta inserir o nome apropriado (p.ex. www.yahoo.com) e o DNS achará o endereço IP real.

Forwarder DNS no WinRoute

O WinRoute está equipado com um módulo DNS que é capaz de encaminhar consultas de DNS a um servidor DNS selecionado na Internet. O módulo DNS armazena os resultados das consultas em seu cache interno onde são mantidos por um certo tempo. Consultas subsequentes repetidas são então respondidas com o uso dos dados no cache sem a necessidade de aguardar pela chegada de uma resposta da Internet.

O forwarder DNS no WinRoute é capaz de responder às consultas de DNS de acordo com o arquivo HOSTS definido pelo usuário. Depois que a consulta de DNS chega o WinRoute procura primeiro no arquivo HOSTS antes de encaminhar a consulta de DNS para a Internet. Se o registro correspondente é encontrado, a consulta é respondida por este valor, se não, é encaminhada ao servidor DNS da Internet.

Servidor proxy

Nesta seção

Visão geral do proxy

O **objetivo principal** de um servidor proxy é **economizar** a **largura da banda** de sua conexão à Internet. Se os usuários têm acesso à Internet através de um servidor proxy, esse servidor pode **armazenar** os vários objetos solicitados que passam por ele (como páginas HTML, imagens e outros tipos de arquivos) em seu **cache**.

Se as páginas ou imagens são novamente solicitadas pelo mesmo usuário ou por algum outro, o servidor proxy fornecerá o item solicitado do seu cache. Isto **reduz** a carga na conexão à Internet e a operação inteira também se torna mais rápida do que fazer novamente um download de imagens da Internet.

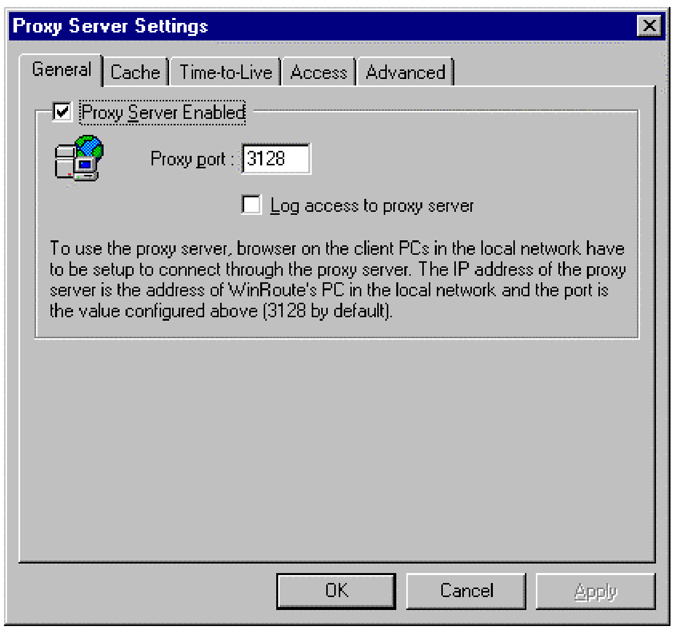
Por outro lado, os objetos armazenados no cache de um servidor proxy ficam desatualizados. Você precisa equilibrar cuidadosamente o **TTL** (Time-To-Live) dos documentos armazenados para evitar mal-entendidos surgidos do fato que você acabou de ler as notícias de ontem da CNN - como um exemplo.

Configuração rápida

Em primeiro lugar - com o WinRoute você **não precisa** que o servidor proxy tenha acesso à Internet. Sua conexão à Internet é mantida por um **roteador NAT** incluído no WinRoute. O NAT é muito melhor para o compartilhamento de acesso à Internet que a tecnologia de servidor proxy. De qualquer maneira o WinRoute também tem um servidor proxy incluído de maneira a oferecer a funcionalidade do armazenamento em quando necessária.

Para iniciar o uso do servidor proxy no WinRoute, siga estes simples passos:

1 Na administração do WinRoute selecione a guia *Configurações -> Configurações do proxy -> Geral*. Marque a opção "Servidor proxy habilitado". Mantenha o número original da porta, 3128.



2 Em seu navegador da Internet (Explorer, Netscape, Opera...), vá até as configurações do proxy, escolha a configuração manual do proxy e insira o endereço do PC do WinRoute como o endereço do servidor proxy para os protocolos HTTP, FTP e Gopher. Digite 3128 como o número da porta do proxy para todos os protocolos.

3 Teste a configuração através do acesso de alguma página da Web pelo navegador.

Guia Propriedades gerais

Servidor proxy habilitado

Use isto para ativar ou desativar o servidor proxy.

Número da porta

O número da porta na qual o servidor proxy espera escutar as solicitações. Normalmente, não há necessidade de mudar o número default, 3128.

Acesso do log ao servidor proxy

Com esta opção habilitada, todas as URLs solicitadas ao proxy pelos navegadores são registradas em um log.

Controle de acesso do usuário

O servidor proxy do WinRoute permite que o administrador controle o acesso à páginas da Web. O administrador pode decidir que os acessos a determinadas páginas ou domínios da Web só podem ser permitidos para determinados usuários e/ou grupos de usuários.

Obrigando os usuários a usarem o servidor proxy

Se você decidir usar o controle de acesso do proxy, você precisa bloquear o acesso direto às páginas da Web, de forma que o acesso através do proxy seja a única alternativa restante para a navegação pela Internet. Para bloquear o acesso direto, defina uma regra de filtragem de pacotes. Para informações sobre filtragem de pacotes, consulte a seção ***Filtro de pacotes*** (see "Obrigando usuários a usarem o servidor proxy" on page 100) do guia do usuário do WinRoute.

Configurando o controle de acesso do proxy

Para configurar o controle de acesso do proxy do WinRoute, vá até a guia "Acesso" nas Configurações do servidor proxy

Lista de acesso

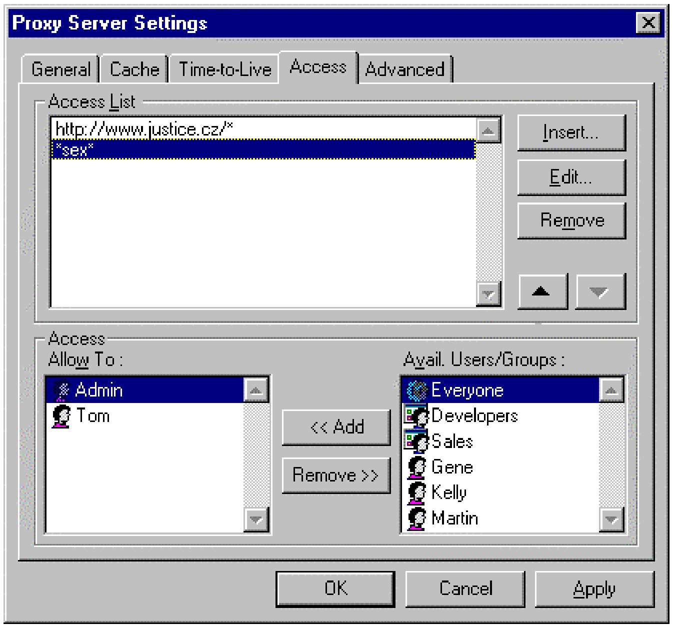
A lista de URLs que são restritas. Você pode usar um asterisco como um curinga para a URL. Por exemplo, para abranger todos os computadores em algumdomínio.com, use a expressão "*.algumdomínio.com". O WinRoute 4.0 também usa a verificação de pedaços de expressões para abranger as URLs, como por exemplo a expressão "sex" abrange o mesmo conjunto de URLs que a expressão "*sex*" (apenas a última variante é suportada em versões anteriores do WinRoute)

Permitir para

A lista de usuários e/ou grupos de usuários que têm permissão de acesso a uma URL em particular.

Usuários/Grupos disponíveis

A lista de usuários e grupos definidos no WinRoute.



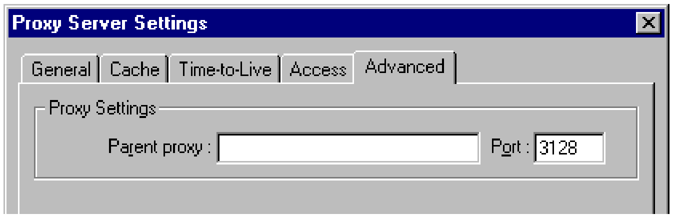
Se um usuário tenta o acesso a uma página da Web que está na categoria de páginas restritas, será solicitado a proceder com uma autenticação pelo seu navegador. O WinRoute verificará se o nome e a senha do usuário estão corretos e se o usuário tem permissão para o acesso à página da Web especificada.

O navegador armazena o nome e a senha do usuário em sua memória. Todas as solicitações de autenticação subsequentes serão respondidas automaticamente de forma que o usuário não tenha que informar repetidamente o seu nome e sua senha.

Por outro lado, os usuários devem ser prevenidos deste recurso. Se você informou seu nome de usuário e sua senha em algum momento durante sua sessão no navegador, deve encerrar a execução do navegador ao deixar o computador para remover os dados de sua autenticação da memória.

Propriedades avançadas

Na guia "Avançado" das configurações do servidor proxy, você pode instruir o WinRoute a usar um servidor proxy pai.



Algumas vezes, você pode ter acesso a um servidor proxy que tem um (consideravelmente) **enorme cache** ou que tem uma conexão **rápida** com a Internet e a sua conexão com esse servidor também é razoavelmente rápida, possivelmente usando uma ligação adicional, além da que você usa normalmente para a sua conexão à Internet.

Para melhorar o ritmo de transferência de dados, você pode decidir que o proxy do WinRoute deve encaminhar todas as solicitações para este servidor proxy pai. Para fazer isto, simplesmente insira o nome e o número da porta do **Proxy Pai** nos campos da guia "**Avançado**".

Sobre o cache

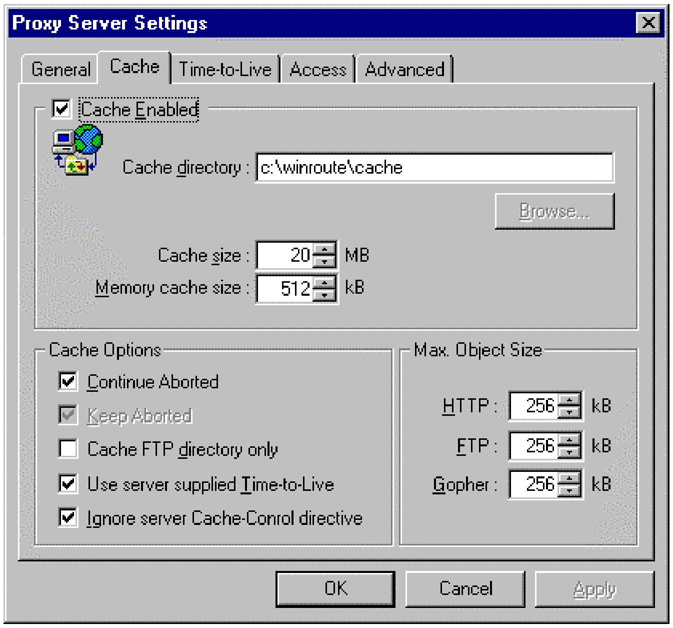
O servidor proxy do WinRoute usa uma maneira **muito econômica** de armazenar dados. Todos os objetos do cache são em **um arquivo de tamanho fixo**. De maneira contrastante, a abordagem normalmente usada por muitos servidores proxy é armazenar cada objeto em um arquivo separado.

Se o disco usa **grandes unidades de alocação** (como FAT16), este método resulta em um **substancial desperdício** de espaço em disco porque os componentes de páginas da Web, em grande parte, são bem pequenos. Normalmente, 50% dos objetos são menores que 6 KB, enquanto o tamanho da unidade de alocação em um disco grande é de 32 KB (com o sistema de arquivo FAT).

O fato é que o cache do WinRoute armazena dados em um único arquivo e ter todos os objetos do cache em um arquivo economiza um grande espaço em disco - até 10 vezes menos espaço é necessário quando comparado à abordagem usual. Isto significa que você precisa de menos espaço em disco ou pode usar o mesmo espaço mais eficientemente.

O arquivo único com tamanho fixo também permite que o WinRoute use técnicas eficientes de indexação que fazem o cache no WinRoute muito rápido.

Configurações do cache



Cache habilitado

Habilita ou desabilita o cache. Se for desabilitado, cada página da Web é sempre carregada diretamente da Internet.

Diretório do cache

O diretório no qual o cache será armazenado.

Tamanho do cache

O montante de espaço em disco que será usado pelo cache do proxy. Quando da decisão sobre o tamanho, considere o número de seus usuários, o tráfego que eles geram, etc. Se você tiver bastante espaço livre você pode definir um cache maior. O tamanho máximo é de3072 megabytes (3 GB).

Continuar mesmo se interrompido

Se marcada, o servidor proxy sempre fará o download de um objeto da Internet até o fim, mesmo se o navegador do usuário cancelar a solicitação (o usuário clica no botão parar, ou segue um link para outra página sem esperar o término do download completo da página atual). Visitas subsequentes à mesma página serão, dessa forma, mais rápidas.

Guardar mesmo se interrompido

Isto instrui o servidor proxy do WinRoute a guardar objetos no cache objetos, mesmo incompletos (páginas da Web, imagens). Isto fornece ao menos um pequeno aumento na velocidade quando a página é visitada novamente. Se a opção "Continuar mesmo se interrompido" estiver marcada, a opção "Guardar mesmo se interrompido" é ignorada.

Guardar no cache apenas o diretório de FTP

Quando da navegação por servidores de FTP, use esta opção para guardar no cache apenas as listagens de diretórios. Se você também quiser armazenar no cache os arquivos transferidos por download de um servidor de FTP, desmarque esta opção. A decisão sobre guardar no cache um arquivo em particular também depende de seu tamanho, consulte o "Tamanho máximo do objeto" abaixo.

Usar o tempo de vida fornecido pelo servidor

O tempo de vida (Time-to-Live, TTL) é o período de tempo após o qual uma determinada página da Web é considerada obsoleta e seu conteúdo deve ser atualizado a partir de seu servidor. Esta opção instrui o servidor proxy do WinRoute a respeitar o tempo de vida (Time-to-Live, TTL) que vem com as páginas individuais. Se uma página não tiver qualquer TTL, será usado o TTL default do proxy.

Ignorar as diretrizes de controle de cache do servidor

Se o conteúdo de uma página da Web muda com muita freqüência, o autor da página pode decidir pela definição de uma diretriz "sem cache" para essa

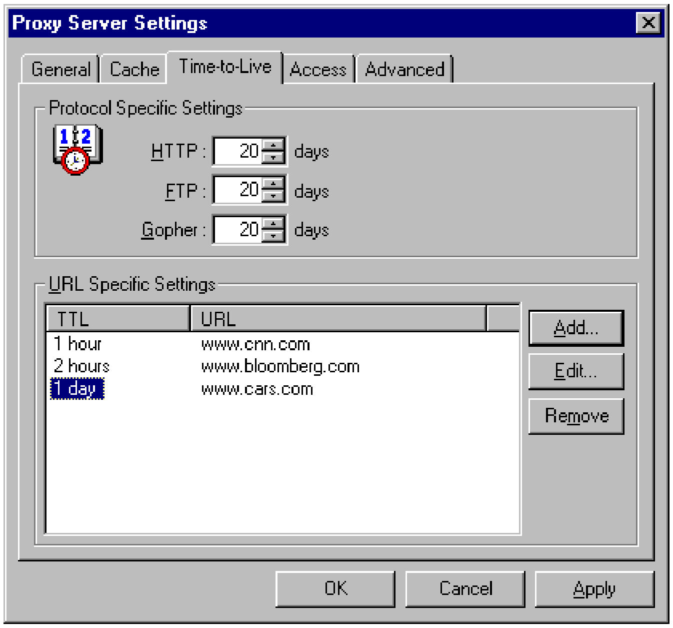
mesma página. Isto é um recurso muito útil, por mais que alguns sites da Web também usem a diretriz com muita freqüência, algumas vezes para todas as suas páginas, eliminando efetivamente o propósito dos servidores proxy. Se você precisar se proteger de um comportamento como este, habilite esta opção.

Tamanho máximo do objeto

O tamanho máximo de objetos a serem armazenados no cache. Objetos maiores serão passados para o navegador do usuário, mas não serão gravados no cache. Normalmente você não precisa guardar grandes objetos no cache (como arquivos de instalação de programas), uma vez que você não faz o download deles repetidamente.

Tempo de vida (time-to-live)

Você pode definir os valores default do Time-to-Live (TTL) que são usados se uma página da Web não tiver qualquer TTL definido para si mesma ou se você decidir ignorar os valores de TTL fornecidos pelo servidor (veja a opção "Usar o tempo de vida fornecido pelo servidor" na guia Cache).



Configurações específicas do protocolo

Aqui você pode definir o TTL default em dias para os protocolos HTTP, FTP e Gopher.

Configurações específicas da URL

Se você precisa definir TTLs individuais para alguns domínios, servidores da Web ou páginas individuais, ponha aqui os valores para as URLs individuais. Você pode definir o TTL em dias e/ou horas.

Você pode usar um asterisco como um curinga na URL. Como um novo recurso no WinRoute 4.0, também é usada a verificação de pedaços de expressões para abranger as URLs, dessa forma você pode digitar apenas "ftp" para abranger todos os servidores que tenham "ftp" em seu nomes. Anteriormente, era necessário que você digitasse "*ftp*" para conseguir esta abrangência.

Observe que se você tem a opção "Usar o tempo de vida fornecido pelo servidor" na guia Cache habilitada, o TTL fornecido pelo servidor tem maior prioridade que as "Configurações específicas da URL".

Como obrigar os usuários a usarem o proxy e não o NAT?

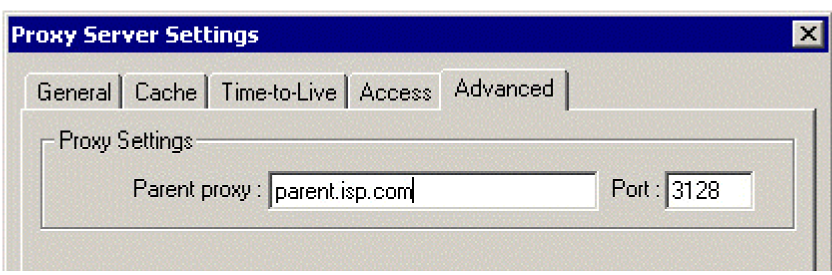
Mesmo que o **NAT** dê a você um excelente capacidade de conexão à Internet, algumas vezes você pode achar de grande utilidade obrigar os usuários a usarem o **Servidor proxy** para fazer o acesso à **World Wide Web**. Normalmente, isto ocorre quando você tem um acesso de 56K para toda a empresa e o cache se torna muito útil ou quando você quer **controlar o acesso do usuários** através de um **filtro de URL** embutido.

Para usar um proxy para o acesso à WWW, você tem que configurar todos os navegadores para que usem o servidor proxy. Lembre-se que a porta default do servidor proxy do WinRoute é **3128**. Você pode mudar esta porta se necessário. Os usuários estarão aptos a contornar o proxy e ir diretamente para a Internet através do NAT. Para impedir tal situação você precisará ajustar o Firewall. Veja o exemplo no capítulo ***Configurações do Firewall*** (see "Obrigando usuários a usarem o servidor proxy" on page 100).

Usando um servidor proxy pai

Servidor proxy pai

Em alguns casos, você precisará que o servidor proxy do WinRoute se conecte com um servidor proxy de "camada superior", o assim chamado **proxy pai**. Vá ao menu *Configurações / Servidor proxy*, clique na guia *Avançado* e digite o endereço IP e a porta do servidor proxy pai.



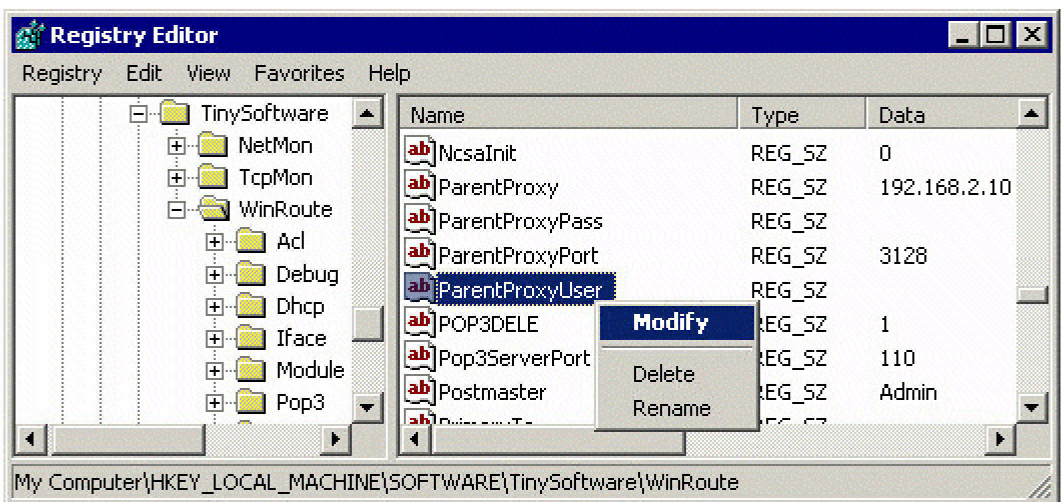
Nome e senha de usuário do proxy pai

O servidor proxy pai poderia exigir a autenticação do usuário para ter acesso a certos (ou todos) sites da Web, de maneira similar a que o WinRoute usa (consulte o capítulo *Controle de acesso do proxy* para detalhes). O WinRoute Pro 4.1 inclui tal autenticação desde a build 22.

Para ativar a autenticação:

- Pare o WinRoute Engine (em Serviços do Windows ou o programa WinRoute Engine Monitor)
- Inicie o Editor de registro do Windows (regedit.exe)
- Encontre a chave *HKEY_LOCAL_MACHINE\Software\TinySoftware\WinRoute*
- No campo da direita, encontre os itens de texto **ParentProxyUser** e **ParentProxyPass** e altere seus conteúdos para o nome de usuário e senha apropriados.
- Feche o Editor de registro e inicie o WinRoute Engine.

Após este procedimento o servidor proxy do WinRoute autenticará a si próprio no servidor proxy pai.



Servidor de correio

Nesta seção

Sobre o servidor de correio do WinRoute

O WinRoute tem um servidor de correio SMTP/POP3 completo embutido. Você pode usá-lo da mesma maneira que usaria o servidor de correio de seu provedor de acesso (ISP). O servidor de correio do WinRoute dá a você a habilidade de enviar e-mail para a Internet e para usuários locais dentro de sua rede. Também permite o recebimento do e-mail e o armazenamento nas caixas de correio dos usuários do WinRoute. O WinRoute também inclui um agendador que permite a você programar a troca de mensagens.

Se você não usar o servidor de correio

Não é necessário usar o servidor de correio do WinRoute. Você pode continuar usando o servidor de correio de seu provedor de acesso (ISP) ou de um terceiro. Nesse caso, o WinRoute atuará como o roteador/firewall que permitirá ao seu software cliente de correio eletrônico a se comunicar com o servidor de correio do seu provedor de acesso.

➢ ***Observe! Não configure o seu software cliente de correio eletrônico para usar o proxy! Você deve usar o NAT do WinRoute para acesso à Internet e configurar o seu software cliente para ter um acesso direto à Internet. Sua incapacidade de estabelecer a troca de mensagens significa que o NAT não está configurado apropriadamente. Consulte a*** Lista de verificação ***de acompanhamento para configurá-lo apropriadamente.***

Contas de usuário

Nesta seção

Sobre as contas de usuário

WinRoute - Contas de usuários

O WinRoute pode ser programado com contas de usuários individuais que podem ser agrupadas (configurado através da guia Configurações | Contas… | Usuários). Os usuários existentes do Windows NT/2000 podem ser importados através da guia Avançado sob o menu Configurações | Contas… .

O que é um usuário

Como um usuário do WinRoute você pode participar em sua administração, ter uma caixa de correio e participar nas políticas de restrição de acesso do proxy do WinRoute.

Os usuários podem criar grupos e aplicar a esses os privilégios ou restrições mencionados acima.

Adicionando um usuário

Para adicionar um usuário:

1 Vá ao menu **Configurações->Contas**

2 Pressione o botão **Adicionar**

3 Defina um **nome de usuário** e uma **senha**

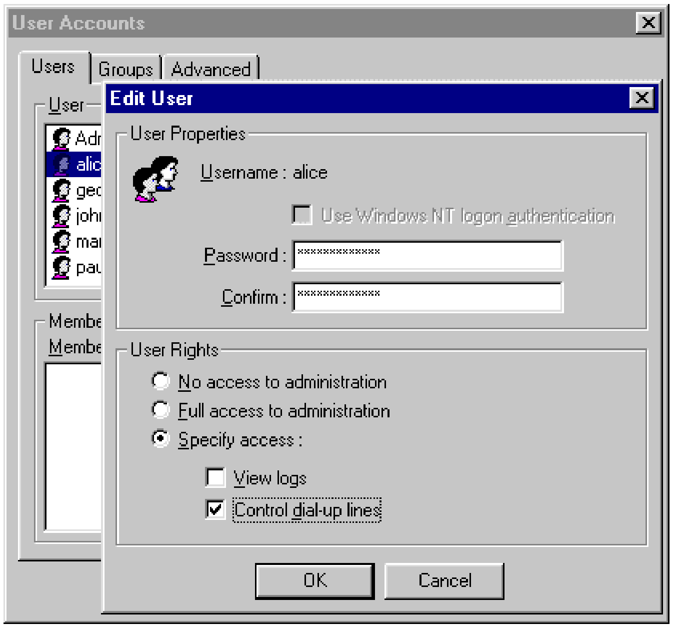
4 Atribua **direitos** ao usuário:

O usuário não tem direito para administrar o WinRoute.

O usuário tem pleno acesso à administração

- **Visualizar logs:** O usuário tem o direito de se conectar ao administrador do WinRoute e de ver apenas as janelas de logs (informações de depuração, log do proxy, log de mensagens, etc.). O usuário não tem o direito de alterar as outras configurações.

- **Controlar linhas de discagem:** O usuário tem o direito de se conectar ao administrador do WinRoute e de estabelecer – desconectar a conexão à Internet. O usuário não tem o direito de alterar as outras configurações.



Grupos de usuários

No WinRoute você pode agrupar usuários em grupos diferentes. Um usuário pode ser um membro de mais de um grupo simultaneamente.

Você deve atribuir **direitos** ao grupo.

➢ ***Observe: os direitos atribuídos a um grupo "substituem" os direitos atribuídos a um usuário.***

O membros de um grupo podem ter os seguintes **direitos**:

O usuário não tem direito para administrar o WinRoute.

O usuário tem pleno acesso à administração.

- **Visualizar logs:** O usuário tem o direito de se conectar ao administrador do WinRoute e de ver apenas as janelas de logs (informações de depuração, log do proxy, log de mensagens, etc.). O usuário não tem o direito de alterar as outras configurações.
- **Controlar linhas de discagem:** O usuário tem o direito de se conectar ao administrador do WinRoute e de estabelecer – desconectar a conexão à Internet. O usuário não tem o direito de alterar as outras configurações.

Administração remota

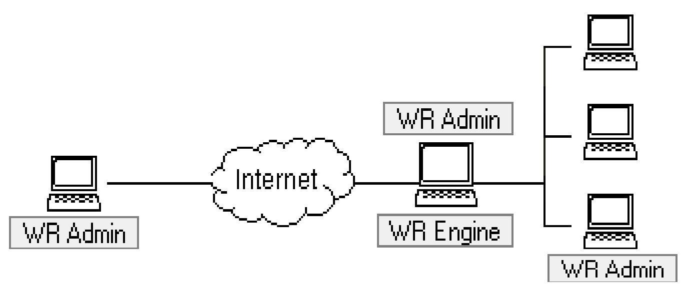
O WinRoute Pro fornece aos usuários o benefício da administração remota. Com as configurações e os direitos apropriados é possível administrar de forma segura o seu firewall de qualquer lugar no mundo. O acesso ao Engine é feito de forma segura por forte criptografia e senha.

Os componentes do WinRoute Pro

O WinRoute Pro 4.x é composto de três módulos:

WinRoute Engine executa todas as operações de roteamento e análise (NAT, filtragem de pacotes, mapeamento de portas, etc.). Você pode Iniciar/Parar o WinRoute Engine a partir do WinRoute Engine Monitor ou, se estiver executando sob o Windows NT, diretamente a partir da opção de serviços do NT. O WinRoute Engine executa de forma invisível como um serviço sob o Windows2000/NT/98 ou 95.

WinRoute Engine Monitor é a aplicação de monitoramento que mostra se o WinRoute Engine está funcionando ou não. Ele aparece como um pequeno ícone azul no canto inferior direito de sua área de trabalho.



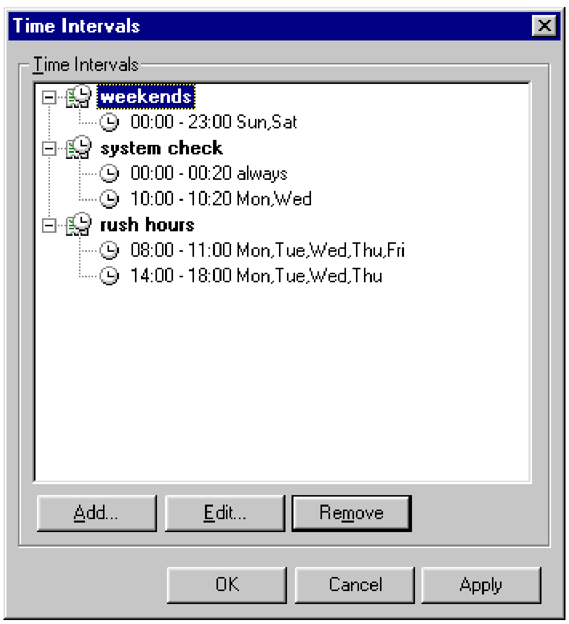
WinRoute Administrator fornece a configuração e os ajustes do WinRoute Engine. O WinRoute Administrator é uma aplicação independente (wradmin.exe) que pode ser executada em qualquer computador e se comunicar através de um conexão TCP/IP com um computador do WinRoute Engine. Para saber as configurações necessárias no WinRoute Engine para permitir a conexão remota consulte os outros capítulos desta seção.

Intervalos de tempo

Você pode definir Zonas de tempo – intervalos de tempo predefinidos – para executar determinadas ações. Estas ações podem ser:

- Filtragem de pacotes
- Troca de mensagens de correio eletrônico (enviar e receber)
- Conexão à Internet
- Configurações avançadas do NAT

A Zona de tempo é um grupo de intervalos de tempo. Como resultado você pode criar um espaço de tempo não homogêneo consistindo de diversos intervalos de tempo.



- ***Exemplo: Você pode criar uma zona de tempo chamada “Dias de descanso e noites” que irá abranger: Sábados, Domingos, Segundas das 16 hs às 6 hs, Terças das 17 hs às 7 hs***

Para definir uma zona de tempo:

1 Vá ao menu *Configurações=>Avançadas=>Intervalos de tempo*

2 Dê um nome à zona de tempo

3 Adicione a nova zona de tempo

CAPÍTULO 2

PREPARAÇÃO E EXECUÇÃO

Neste capítulo

Requisitos do sistema

Para instalar e executar o WinRoute Pro 4.1 nos recomendados como configuração mínima:

- PC de categoria Pentium (um ou dois processadores)
- Sistema operacional Windows 95/98/NT4.0/2000
- Memória RAM de 32MB
- 1MB de espaço livre em disco
- mínimo de 2 interfaces disponíveis. Estas podem ser: Ethernet, RAS, TokenRing, DirecPC

Lista de verificação rápida

Para todos os usuários do WinRoute existe a lista básica de configurações e regras que, se executada, garante uma conexão bem sucedida de sua rede com a Internet. É evidente que a existência de uma conexão à Internet sem problemas é imprescindível.

Você deverá efetuar as configurações descritas abaixo se desejar o benefício de usar o NAT para compartilhar o acesso à Internet. Se você deseja usar um servidor proxy (embutido no WinRoute) não precisa efetuar estas configurações. Nesse caso você precisaria apontar os seus navegadores e aplicações para o servidor proxy do WinRoute. Recomendamos expressamente o uso do NAT (Network Address Translation) sempre que possível. É mais rápido, seguro e confiável.

Configurações e regras

1. **No PC com WinRoute - duas interfaces (placas de rede)**
   Certifique-se de que o computador do WinRoute tem (no mínimo) duas interfaces. Uma para a conexão com a Internet e outra para a conexão local/cliente. Elas podem ser placas de rede ou linhas do RAS. Uma interface (Ethernet ou RAS/discagem) é usada para a conexão com a Internet enquanto a(s) outra(s) interface(s) (Ethernet, token ring…), para a conexão com a(s) sua(s) rede(s).

2. **Assegure-se de poder "pingar" em todos os endereços IP!**
   Para fazer o WinRoute funcionar de forma adequada, as máquinas clientes precisam estar aptas a "pingar" os endereços IP públicos e privativos da máquina host do WinRoute.

3. **No PC com WinRoute - habilite o NAT na interface com a Internet!**
   Certifique-se que o NAT está marcado como ON para a interface de conexão com a Internet (Ethernet, linha do RAS). Configure isto no menu **Configurações=>Tabela de interface** e vá para as propriedades da interface desejada.

4 No PC com WinRoute - desabilite o NAT na interface interna!
Certifique-se que o NAT está **DESMARCADO** na interface(s) que se conecta(m) com a rede interna.
Observe! Em configurações muitos específicas o NAT pode estar marcado como "ON" mesmo na interface interna. Você pode ver este exemplo aqui (quando disponível).

5 No PC com WinRoute - sem Gateway na interface interna!
Certifique-se de que NÃO há gateway default nas propriedades de rede da interface (placa de rede) de conexão com a rede interna. É evidente que o gateway default na interface de conexão com a Internet será configurado de acordo com os detalhes fornecidos pelo seu provedor de acesso (ISP).

6 No PC com WinRoute - insira as opções na configuração do DHCP!
Na maioria dos casos você usará o servidor DHCP do WinRoute para uma configuração automática da rede. Verifique duas vezes se você definiu o(s) escopo(s) dos endereços IP que você deseja que o servidor DHCP atribua junto às Opções. Nas Opções você pode especificar outras informações dadas para as suas estações - como servidor DNS, gateway default, etc.

7 No PC cliente - o endereço IP interno do PC do WinRoute é o gateway default!
O PC do WinRoute age como o GATEWAY DEFAULT de todos os computadores na rede local (LAN). Como resultado, use o endereço IP da placa de rede interna no host do WinRoute (p.ex.192.168.1.1) como o gateway em todos os computadores internos/clientes. Configure este valor em cada computador "cliente" OU configure apenas uma vez no servidor DHCP do WinRoute e ele atribuirá este valor às suas estações automaticamente! Consulte os Exemplos de redes (interligação de) mais avançadas se precisar usar um gateway default diferente!

8 No PC cliente - verifique o DNS!
Na maioria dos casos você usará o forwarder DNS embutido no WinRoute como um servidor DNS dos seus computadores da rede. Certifique-se que o forwarder DNS embutido do WinRoute esteja ativo (ON) e configurado. Você pode usar o endereço do servidor DNS do seu provedor de acesso (ISP) inserindo-o diretamente nos campos apropriados na configuração TCP/IP de cada computador da rede.

- ***Nos casos em que o WinRoute é usado apenas como um Firewall ou Servidor de correio (p.ex. sem solicitação de compartilhamento de acesso à Internet), NÃO é necessário ativar ("ON") o NAT para qualquer interface.***

- ***As interfaces no computador do WinRoute devem ter endereços IP diferentes de redes diferentes. Não é possível atribuir endereços IP da mesma rede às interfaces (p.ex. 207.181.216.23 em uma e 207.181.216.24 na outra). O mais comum é que você tenha uma interface local (LAN) e outra para a Internet. Você não terá qualquer problema. No caso de você ter três interfaces (2 locais e uma para a Internet) deve atribuir endereços IP de redes diferentes às interfaces locais (uma 192.168.1.1 e a outra 192.168.2.1).***

Software conflitante

Existem diversas questões conhecidas sobre softwares incompatíveis:

Norton Antivirus

Desabilite a porta 110 na configuração do Norton Antivirus se desejar usar o servidor de correio do WinRoute. Manter a porta 110 no Norton fará com que o computador não inicie.

WinGate

Desinstale o WinGate antes da instalação do WinRoute. Desinstale tanto o servidor quanto o cliente.

SyGate

Desinstale o SyGate antes da instalação do WinRoute. Desinstale tanto o servidor quanto o cliente.

MS Proxy Server

Desinstale o MS Proxy Server antes da instalação do WinRoute. Desinstale tanto o servidor quanto o cliente. Remova o TCP/IP, reinicie e adicione o protocolo novamente.

Microsoft Internet Connection Sharing

Desinstale o MS ICS antes da instalação do WinRoute, remova o protocolo TCP/IP, reinicie e adicione o protocolo novamente.

WinProxy da Ositis

Desinstale o WinProxy antes da instalação do WinRoute, remova o protocolo TCP/IP, reinicie e adicione o protocolo novamente.

Todos os softwares mencionados acima, estão usando drivers que não funcionam de forma apropriada com as camadas inferiores do protocolo de rede operado pelo WinRoute.

Questões com a tabela de roteamento

É possível que você tenha instalado e configurado todos os componentes com êxito e ainda assim continue tendo problemas de funcionamento. Infelizmente o sistema operacional Windows 95/98/NT não foi bem projetado para comunicação em rede. Mesmo após configurar o WinRoute e a rede corretamente você pode sentir que essa configuração não está funcional. Se este for o caso, você tem que examinar a tabela de roteamento e escolher um das seguintes opções:

- acertar as rotas excluindo-as e, em seguida, adicionando-as - apenas para usuários experientes

ou

- remover o protocolo TCP/IP completamente, dar um novo boot na computador e adicionar o protocolo novamente. O desempenho é garantido.

Questões com o software cliente do proxy

Alguns servidores proxy exigem a instalação de um software em todas as máquinas clientes. Este software cliente faz com que as aplicações consultem um servidor proxy. Se o software cliente do proxy não for removido, pode ocorrer dessa máquina não se conectar à Internet porque o WinRoute não está configurado como um servidor proxy. Se o cliente ainda não conseguir se conectar à Internet, reinstale o TCP/IP, refaça as suas configurações e dê um novo boot na máquina.

Questões com drivers de placa de rede

Tente usar as placas de rede mais próximas do padrão. Se você tiver uma placa especial, velha ou bem nova em seu computador, seu driver pode incluir instruções específicas que impedirão que o WinRoute se comunique com ela. Tente encontrar a placa Ethernet mais próxima do padrão em sua rede e simplesmente troque-as de lugar. Um bom número de clientes "tristes" ficaram "felizes" apenas por trocar a placa ou atualizar o driver.

O WinRoute é um software de roteador/firewall completamente neutro que não exige qualquer software cliente em execução nos computadores clientes a menos que seja usada a administração remota. Nesse caso a Administração do WinRoute (wradmin.exe) deve ser instalada em uma máquina cliente ou externa.

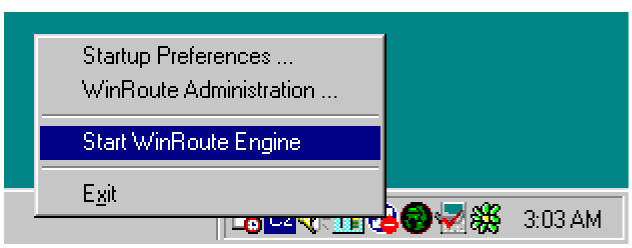
Administração no WinRoute

Nesta seção

Administração a partir da rede local

Para administrar o WinRoute a partir da rede local ou do computador com o WinRoute você deve fazer o seguinte:

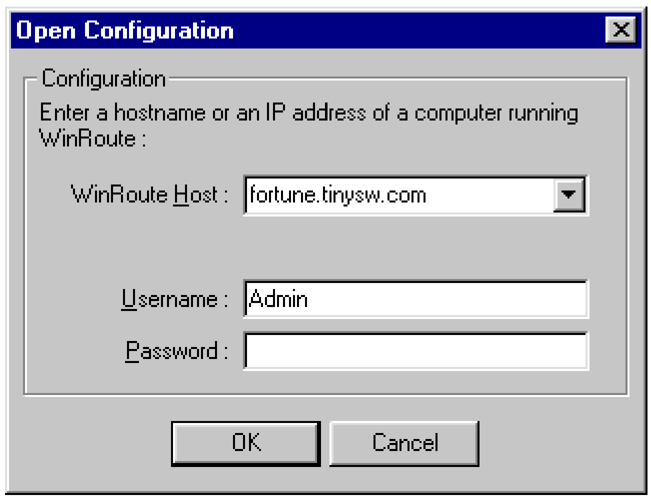
1. **Verifique se o WinRoute Engine está ativo e em execução**
   Para verificar se o WinRoute foi iniciado, execute o WinRoute Engine Monitor a partir do grupo de programas do WinRoute 4.0. Um pequeno ícone redondo, azul e branco, será exibido na bandeja do sistema na barra de tarefas canto inferior direito da área de trabalho). Isto indica que a aplicação está sendo executada. Uma cruz vermelha sobre o ícone indica que o WinRoute está parado. Para iniciar o WinRoute Engine simplesmente **clique com o botão direito do mouse** no ícone e escolha Iniciar o WinRoute Engine a partir do menu pop-up.



2. Inicie o WinRoute Administrator

Para iniciar o módulo de administração do WinRoute, execute a aplicação a partir do menu Iniciar=>Programas=>WinRoute 4.0 ou clicando com o botão direito do mouse o ícone do WinRoute Engine Monitor e escolhendo *Administração do WinRoute* a partir do menu pop-up. Você também pode copiar o arquivo *WRAdmin.exe* para qualquer outro computador em sua rede e executá-lo a partir de lá.

Quando a janela Admin é exibida, você deve deixar o host local predefinido ou insira o endereço IP do computador no qual o WinRoute está sendo executado. Informe o nome de usuário e a senha usada para administração.



Observação: Ao conectar pela primeira vez, você pode usar "Admin" como o nome do usuário e deixar a senha em branco. Veja a Configuração de usuário para detalhes adicionais com respeito à política de nome de usuário e senha de administração.

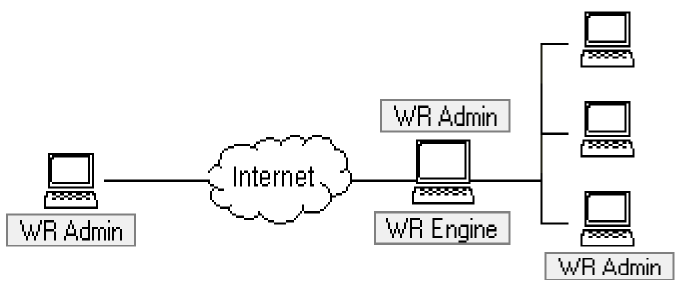
Você tem que efetuar um login bem sucedido como Administrador no WinRoute Engine para efetuar configurações.

Possíveis razões para um login mal sucedido a partir de uma rede local:

- O WinRoute Engine não está ativo e em execução
- Nome do usuário e senha errados
- Endereço IP informado na conexão com o WinRoute Engine está incorreto
- Você não tem direitos de administrador do WinRoute
- Você tem o NAT ativo na interface de conexão com a sua rede – consulte a lista de verificação e o capítulo Configurando a rede desta ajuda

Administração a partir da Internet

Você pode administrar o WinRoute Pro Engine a partir de qualquer computador no mundo contanto que haja uma conexão TCP/IP no local. A administração é segura (criptografada) e controlada através do uso de um nome de usuário e uma senha.



Para administrar o computador do WinRoute de fora da rede (da Internet, por exemplo) o apeamento de porta precisa estar configurado no computador do WinRoute. Você deve entender que com o NAT ativo (ON) na interface de conexão à Internet (necessário para o compartilhamento de conexão à Internet), a sua rede inteira, incluindo o computador do WinRoute, está totalmente protegida e, portanto, ninguém tem acesso a ela.

Para configurar o mapeamento de porta para a administração remota vá ao menu *Configurações=>Avançadas=>Mapeamento de porta*, pressione adicionar e defina:

Protocolo: TCP/UDP

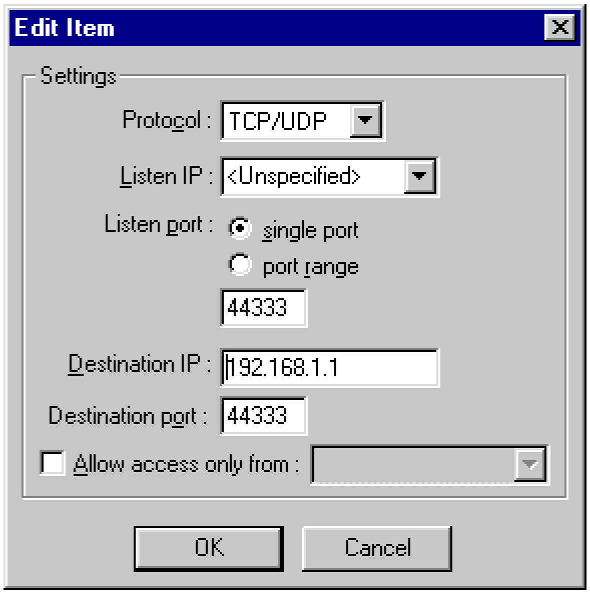
IP de escuta: <não especificado> (recomendado) ou o endereço IP da interface.

Porta de escuta: 44333

IP de destino: o endereço IP da interface de conexão do computador do WinRoute à rede local (endereço IP de classe privativa)

Porta de destino: 44333

Permitir acesso apenas de: Se esta opção estiver marcada você poderá limitar o acesso ao WinRoute Engine. Você precisar predefinir os endereços IP com permissão para ter acesso ao WinRoute Engine a partir da Internet no menu *Configurações=>Avançadas=>Grupos de endereços*. Você agrupar endereços IP separados, faixas de endereços IP e redes.



Veja exemplos para maiores detalhes sobre mapeamento de porta. Se você estiver com tudo configurado de acordo, simplesmente execute o programa de administração do WinRoute a partir de qualquer computador e insira o endereço IP (registrado - p.ex. 206.86.181.25) do computador no qual o WinRoute está sendo executado e, além disso, o nome de usuário e a senha usados para a administração naquele computador. Consulte a configuração de usuário para detalhes adicionais com respeito à política de nome de usuário e senha para administração.

Possíveis razões para um login mal sucedido a partir da Internet:

- O WinRoute Engine não está ativo e em execução
- Nome do usuário e senha errados
- Endereço IP informado na conexão com o WinRoute Engine está incorreto
- Você não tem direitos de administrador do WinRoute

- O mapeamento de porta está errado ou não está configurado no computador no qual o WinRoute Engine está sendo executado

Perda da senha do administrador

Se você perder a senha de administração envie o e-mail para support@tinysoftware.com para instruções adicionais. Por razões de segurança não publicamos a solução para este problema.

Configurando a rede

Nesta seção

Sobre o DHCP

Com o uso do servidor DHCP você pode simplificar significativamente a configuração das estações dentro de sua rede. Ao usar o servidor DHCP a única configuração que você precisa fazer nas estações clientes é que elas obtenham dinamicamente um endereço IP do servidor DHCP. (Esta configuração é um default quando da adição do protocolo TCP/IP nas propriedades da rede.)

➢ ***Você pode usar o servidor DHCP embutido no WinRoute ou qualquer um servidor de terceiros dentro de sua rede. Certifique-se de que apenas um servidor DHCP esteja sendo executado em sua rede ao mesmo tempo!***

Visão geral do gateway default

O WinRoute age como um roteador. Como tal ele exige duas configurações básicas do TCP/IP em cada computador de sua rede:

- Atribuir endereço IP – manualmente ou através do servidor DHCP (p.ex. servidor DHCP do WinRoute)
- Definir o gateway default

O **gateway default** em cada computador que tem acesso à Internet através do computador do WinRoute; deve ser definido para o **endereço IP** da interface Ethernet do computador do WinRoute que se conecta com a rede (LAN).

Exemplo:

O computador cliente tem o endereço IP 10.10.10.23 enquanto o PC do WinRoute tem duas interfaces, uma de conexão ao modem a cabo (cable modem) com um IP do provedor de acesso (como 203.23.14.232) e uma outra de conexão à rede privativa (10.10.10.1). O gateway default no computador 10.10.10.23 será definido como 10.10.10.1.

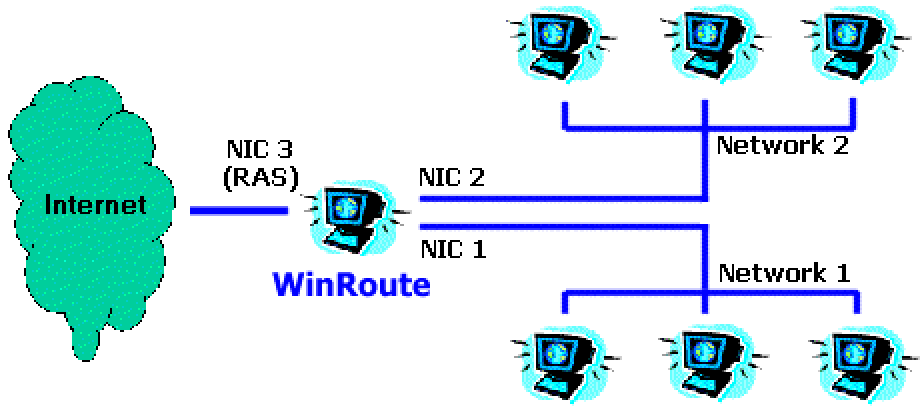
- ***Observação 1: Ao criar o espaço de endereço IP dentro de sua rede local você deve usar o endereço IP da mesma sub-rede. Por exemplo, se a máscara de sub-rede que você usa é 255.255.255.0 então todos os endereços devem ser de 10.10.10.1 a 10.10.10.255.***

- ***Observação 2: Você pode mais redes conectadas à Internet através do WinRoute. Você pode ter mais interfaces no computador do WinRoute, uma para cada rede. Então cada uma destas interfaces (seu endereço IP) representa o gateway default para o resto da rede conectada a elas.***

Escolhendo o computador correto para o WinRoute

O WinRoute **DEVE SEMPRE** ser executado no computador que está conectado à Internet - através de uma placa de rede, cabo, modem DSL, linha discada ou um roteador.

O WinRoute sempre atua como o gateway entre duas (ou mais) redes onde cada uma delas é representada por uma interface. Estas interfaces podem ser placas Ethernet, adaptadores RAS, adaptadores USB-para-Ethernet, adaptadores PPPoE, etc.

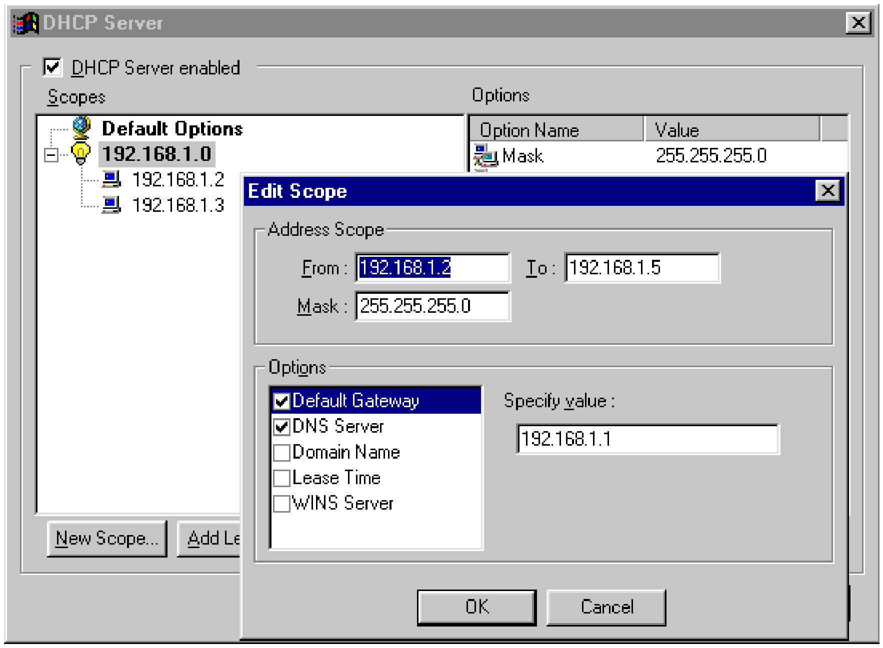

Internet
NIC 3
(RAS)
WinRoute
NIC 2
NIC 1
Network 2
Network 1

Configuração do IP com servidor DHCP

Verifique duas vezes se as suas estações estão configuradas para obter um endereço IP do servidor DHCP (consulte as propriedades em *TCP/IP->interface de rede* de cada computador) e se todas as outras propriedades do TCP/IP estão em branco, incluindo as informações sobre o servidor DNS.

A seguir execute o programa de administração do WinRoute:

1. Vá ao menu *Configurações=>Servidor DHCP*.
2. Habilite o servidor DHCP (marque a opção) e pressione o botão para adicionar um **Novo escopo**.
3. **Adicionar escopo**
   Aqui você irá especificar o escopo de endereços IP usados pelo servidor DHCP que são dados às estações. Lembre-se que um endereço IP já é usado pelo computador do WinRoute e você não deve usá-lo. A faixa de endereços IP precisa ser da mesma sub-rede. Veja a imagem como exemplo.
4. **Especificar opções (importante!)**
   Em Opções você deve especificar que outras informações serão fornecidas às estações (p.ex. gateway default, servidor DNS, etc.). Marque a caixa ao lado de cada componente na caixa de diálogo e insira a informação apropriada. Insira a informação do gateway default e do servidor DNS (tipicamente você pode usar o WinRoute como servidor DNS) e use o endereço IP do computador do WinRoute (p.ex. 192.168.1.1). Você pode deixar as outras opções em branco.


DHCP Server
DHCP Server enabled
Scopes
Options
Default Options
192.168.1.0
192.168.1.2
192.168.1.3
Option Name
Value
Mask
255.255.255.0
New Scope...
Edit Scope
Address Scope
From :
192.168.1.2
To :
192.168.1.5
Mask :
255.255.255.0
Options
Default Gateway
DNS Server
Domain Name
Lease Time
WINS Server
Specify value :
192.168.1.1
OK
Cancel

- ***Observação: O endereço IP da interface Ethernet (de conexão com a rede local) no computador do WinRoute deve estar atribuído e você usará este endereço IP em outros computadores como o gateway default e (opcionalmente) como servidor DNS! De qualquer modo o gateway default naquela interface estará em branco.***

Configuração do IP com servidor DHCP de terceiros

Usar um servidor DHCP de terceiros para a configuração de sua rede requer uma atenção especial aos valores enviados por tal servidor DHCP para as estações clientes dentro de sua rede.

Verifique duas vezes se o seu servidor DHCP está enviando as informações corretas para as suas estações clientes! Isto é, você precisa configurar o servidor DHCP para atribuir a outros computadores o endereço IP da placa de rede do computador do WinRoute como gateway default e (opcionalmente) servidor DNS.

O endereço IP enviado para a estação cliente também deve ser da mesma sub-rede do computador do WinRoute.

VERIFIQUE DUAS VEZES (!!!) se a placa de conexão com a rede interna no computador do WinRoute tem um endereço IP fixo **atribuído** (p.ex. 192.168.1.1) e este endereço é enviado pelo DHCP como o gateway default para o resto da rede. O servidor DHCP pode não atribuir um endereço IP ao host do WinRoute!

Exemplo:

O servidor NT com DHCP está com o endereço 192.168.1.1 enquanto o WinRoute está usando o 192.168.1.5. A informação de gateway default (e DNS se você usar o DNS do WinRoute) enviada para as estações será 192.168.1.5.

Configuração do IP - atribuição manual

Em alguns casos é necessário atribuir manualmente endereços IP às estações. Ao fazer isso, leve em consideração as seguintes regras:

Atribuir endereço IP

Atribua um endereço IP do "tipo interno" (ou privativo) a cada computador. Normalmente 192.168.x.x ou 10.x.x.x. Atribua endereços IP da mesma sub-rede para cada sistema. Por exemplo, uma vez que um endereço IP esteja definido para o host do WinRoute como 192.168.1.1, você deve continuar como mesmo esquema de numeração. (p.ex.192.168.1.2, 192.168.1.3, etc.)

Definir o gateway default

Use o endereço IP do host do WinRoute como gateway default para todos os seus computadores clientes. Em outras palavras, cada computador cliente usará o endereço IP do host WinRoute (endereço IP interno) como o gateway default. Isto é informado nas propriedades da rede do computador em TCP/IP=>Adaptador Ethernet.

Definir o DNS

Finalmente, use o endereço IP do computador do WinRoute como o forwarder DNS para todos os seus computadores (o endereço IP interno, se você estiver usando o servidor DHCP do WinRoute). A única exceção seria ao usar o endereço do DNS do seu provedor de acesso ou outro servidor DNS. Em seguida você informará os detalhes do DNS dados a você pelo seu provedor de acesso (nas propriedades em TCP/IP->Placa de rede de cada estação).

Importante! Consulte o capítulo recomendado deste manual com respeito a configurações adicionais de DNS!

Configurando o forwarder DNS

O servidor DNS é configurado através do menu: *Configurações => Servidor DNS*.

"Habilitar encaminhamento do DNS"

Esta opção controla se o servidor DNS é ativado ou não.

"Encaminhar consultas ao DNS para o servidor selecionado automaticamente pelos servidores DNS conhecidos pelo sistema operacional"

Se selecionado, todas as consultas ao DNS são encaminhadas para o servidor DNS escolhido na configuração do TCP/IP da interface com a Internet ou da rede dial-up

"Habilitar procura no arquivo HOST"

Com esta opção marcada, o servidor DNS tem a permissão de usar dados do arquivo HOSTS ao responder as consultas.

"Editar arquivo HOSTS..."

Este botão ativa um editor de textos externo com o qual você pode editar o arquivo HOSTS.

"Domínio do DNS"

Informe o seu nome de domínio (p.ex. "acme.com") aqui. Ao responder as consultas ao DNS, o nome de domínio é anexado ao nome do host obtido do arquivo HOSTS ou da tabela de liberação do DHCP.

"Encaminhar consultas ao DNS para"

Informe o endereço IP numérico do servidor DNS para o qual você deseja encaminhar as consultas. Escolha um endereço do servidor DNS do seu provedor de acesso ou de um servidor ao qual você tenha um acesso rápido.

"Habilitar cache do DNS"

Isto permite que as respostas às consultas ao DNS sejam armazenadas em um cache interno. Consultas subsequentes são então processadas com o uso do conteúdo do cache, sem esperar por uma resposta do servidor DNS fora de sua rede.

"Ao resolver nome do arquivo HOSTS ou da tabela de liberação combine-o com o domínio DNS"

Este recurso pode ser melhor entendido a partir de um exemplo - você pode desejar resolver a consulta ao DNS do computador JOHN. No arquivo HOSTS você informou que o seu domínio OFFICE está associado com um endereço IP específico. Então a consulta JOHN.OFFICE poderia ser resolvida corretamente.

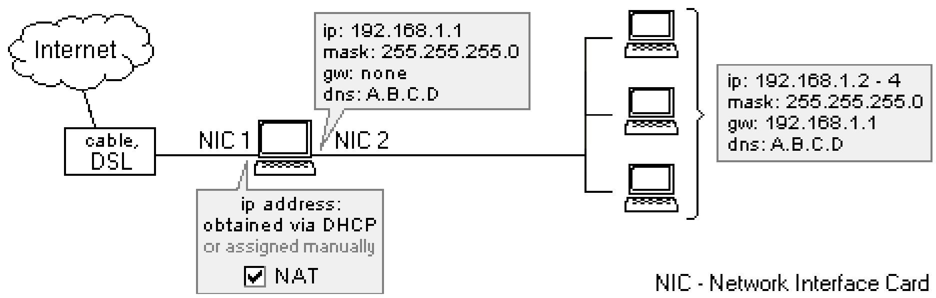
➢ ***Observe que o cache apenas armazena as respostas que são do tipo "Nome => endereço IP". As respostas ficam armazenadas até a sua expiração. O tempo de expiração é fornecido pelos servidores DNS junto com cada resposta.***

Conectando a rede à Internet

Nesta seção

Conexão DSL

Uma conexão DSL (ADSL, SDSL) requer duas placas de rede (NIC) instaladas no computador do WinRoute. Uma fará a conexão com a Internet (modem DSL) enquanto a outra fará a conexão com a rede interna.



Configuração do WinRoute

Para conectar à Internet

1 Vá ao menu Configurações->Tabela de interface

2 Escolha a placa de rede de conexão à Internet, clique em Propriedades e marque a opção "Execute o NAT com o endereço IP desta interface em toda comunicação que passe por ela". Ao abrir a caixa de diálogo da tabela de interface você verá o NAT ativo (ON) ao lado desta linha externa.

3 Certifique-se que o NAT NÃO está ativo (NOT ON) para a interface de conexão com a rede interna (vá às propriedades desta interface na tabela de interface)

4 Certifique-se de que NÃO há gateway definido nas propriedades do TCP/IP da placa de rede interna (vá às configurações da rede) e que há um endereço IP interno atribuído à placa.

5 Certifique-se de que a placa de rede de conexão à Internet foi configurada de maneira apropriada com os dados de seu provedor de acesso. No caso de você ter endereços IP atribuídos dinamicamente deixe as configurações de endereço IP em branco.

Para outras configurações de rede consulte os capítulos apropriados, especialmente a ***Lista de verificação*** .

Conexão PPPoE DSL

PPPoE é uma tecnologia desenvolvida recentemente para muitos assinantes DSL. Embora esteja sendo amplamente disponibilizada por diversos provedores de acesso esta tecnologia provê os usuários com um desempenho inadequado e não é (no momento atual) a melhor solução que você pode ter para a conexão de sua rede à Internet. Os consumidores devem exigir a solução DSL padrão sempre que possível.

A disponibilização do PPPoE com o WinRoute é similar ao DSL padrão em termos de configurações do TCP/IP. O WinRoute Pro pode ser instalado no mesmo computador do adaptador PPPoE. O WinRoute Pro reconhecerá o adaptador PPPoE como uma interface de rede. Você pode habilitar o NAT nesta interface. Você também pode ver o adaptador ethernet (ligado ao modem a cabo) como a interface na tabela de interface do WinRoute Pro. Você não deve habilitar o NAT nessa interface.

O WinRoute Pro funciona perfeitamente com todos os adaptadores PPPoE disponíveis no mercado. Contudo - de vez em quando - os consumidores podem ter problemas de desempenho com certos adaptadores PPPoE:

Enternet 100, 300, 500 PPPoE client

O WinRoute Pro 4.1 trabalha bem com o Enternet PPPoE client da NTS se você tiver ativado o Protocol Driver (driver de protocolo) ao invés do Filter Driver (driver de filtro) default. Para isso você deve executar o Enternet PPPoE client, ir ao menu Settings->Advanced e alterar os valores desejados.

Se você tiver problemas de desempenho pode precisar também reduzir o MTU nas máquinas clientes para 800.

WinPoet da Ivasion

O WinRoute Pro 4.1 trabalha bem com o WinPoet sob as seguintes circunstâncias: com a compressão de cabeçalho IP (é configuração do RAS/Rede dial-up) desativada.

Reduzindo o MTU:

O adaptador PPPoE acrescenta informações adicionais ao cabeçalho de todo pacote de saída. Por default, o windows usa o máximo tamanho permitido de pacote. O adaptador PPPoE equilibra isto ao garantir que o MTU da máquina local esteja levemente reduzido para compensar as informações adicionais acrescentadas a cada pacote. Infelizmente, todas as outras máquinas ainda usam o tamanho máximo para transmissão. Isto resultará em perda de pacotes. Os links a seguir mostrarão a você como reduzir o MTU em todos os clientes.

Para usuários do Windows 95/98:

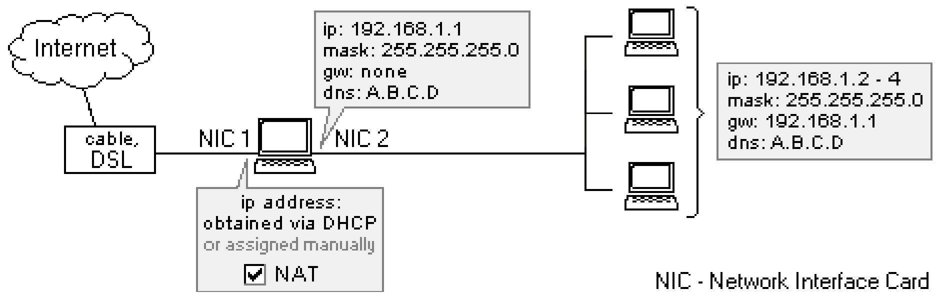
http://www.microsoft.com/support/kb/articles/Q158/4/74.asp

Para usuários do Windows NT4/2000:

http://www.microsoft.com/WINDOWS2000/library/resources/reskit/samplechapters/cnbd/cnbd_trb_vcfx.asp

Conexão com modem a cabo (bidirecional)

A conexão através de modem a cabo requer duas placas de rede (NIC) no computador do WinRoute. Uma placa para a conexão com a Internet (modem a cabo) enquanto a outra será usada na conexão com a rede interna. Para modems a cabo unidirecionais (modem para upload, cabo para download) vá ao capítulo apropriado.



Configuração do WinRoute

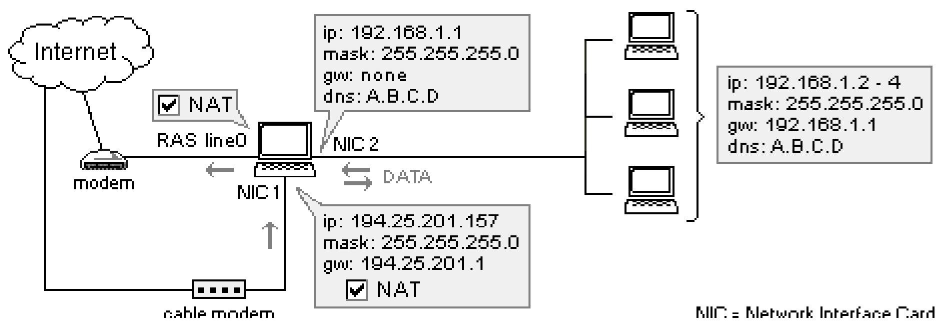
1. Vá ao menu Configurações->Tabela de interface
2. Escolha a placa de rede de conexão à Internet, clique em Propriedades e marque a opção "Execute o NAT com o endereço IP desta interface em toda comunicação que passe por ela". Ao abrir a caixa de diálogo da tabela de interface você verá o NAT ativo (ON) ao lado desta linha externa.
3. Certifique-se que o NAT NÃO está ativo (NOT ON) para a interface de conexão com a rede interna (vá às propriedades desta interface na tabela de interface)
4. Certifique-se de que NÃO há gateway definido nas propriedades do TCP/IP da placa de rede interna (vá às configurações da rede) e que há um endereço IP interno atribuído à placa.
5. Certifique-se de que a placa de rede de conexão à Internet foi configurada de maneira apropriada com os dados de seu provedor de acesso. No caso de você ter endereços IP atribuídos dinamicamente deixe as configurações de endereço IP em branco.

Para outras configurações de rede consulte os capítulos apropriados (p.ex. ***lista de verificação*** , ***Configuração de IP*** , etc.)

Modem a cabo unidirecional (upload pelo modem, download pelo cabo)

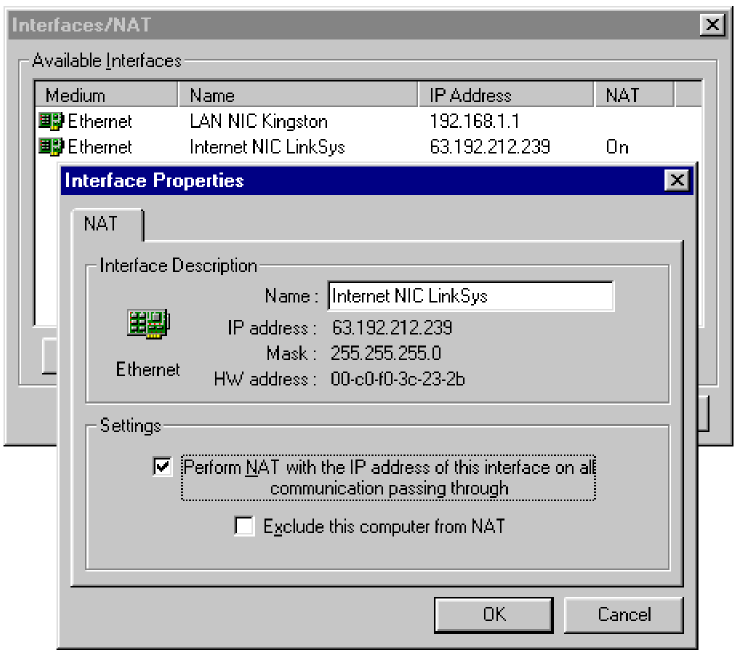
OBSERVAÇÃO: Este tipo de conexão à Internet **não é uma "configuração oficialmente suportada"** uma vez que as configurações **podem variar** de provedor de acesso para provedor de acesso. De qualquer modo, tentamos fornecer soluções de acesso para tantas situações quanto possível. Muitos de nossos usuários têm tido êxito com as configurações a seguir ao tentar estabelecer uma conexão.

Em geral o fluxo de dados é **similar ao Direc PC**. Os pacotes de saída fluem através da sua interface de conexão **discada**. No caminho de volta eles são roteados **através de um cabo**. De fato, o seu provedor de acesso tem que associar as suas duas interfaces ao mesmo tempo. Isto parece complicado mas é a única maneira de estabelecer uma conexão bem sucedida. Por esta razão, aconselhamos verificar junto ao seu provedor de acesso antes de ir em frente com a sua aquisição do WinRoute



1. Vá ao menu *Configurações->Tabela de interface*. Você verá uma interface de **linha do RAS** (seu modem) e duas interfaces de **placa de rede** - uma para conexão com a Internet e outra para conexão com a rede local

2. Clique na interface da placa de rede de conexão com a Internet e vá para *"Propriedades."* Marque a opção *"Execute o NAT com o endereço IP desta interface em toda comunicação que passe por ela."*



3. Clique na **interface do RAS** e vá para *"Propriedades."* Marque a opção *"Execute o NAT com o endereço IP desta interface em toda comunicação que passe por ela"*. Na **guia RAS** selecione a conexão que você usará para o seu provedor de acesso, insira o seu nome de usuário e a senha.

4. Certifique-se que o NAT **NÃO está ativo (NOT ON)** para a interface de conexão com a rede interna (vá às propriedades desta interface)

5. Certifique-se de que **NÃO há gateway** definido nas propriedades do TCP/IP da placa de rede interna (vá às configurações da rede) e que há um **endereço IP** de classe privativa (p.ex.10.10.1.1).

6. Certifique-se de que a placa de rede de conexão à Internet foi configurada de maneira apropriada com os dados de seu provedor de acesso (propriedades do TCP/IP). Observação: No caso de você ter endereços IP atribuídos dinamicamente deixe as configurações de endereço IP em branco.

➢ ***Em geral o NAT deve ser ativado ("ON") em ambas as interfaces de conexão com a Internet - RAS e discada.***

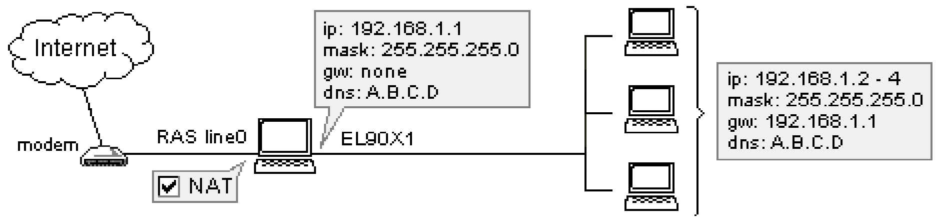
Conexão via linha discada ou ISDN

Conexão via linha discada ou ISDN

Se você tem acesso à Internet por linha discada (56K ou ISDN) em um PC com Win95, Win98 ou NT4.0 , você tem o necessário para executar o WinRoute. O WinRoute precisa ser executado em um computador que tenha:

- modem ligado à linha telefônica ou ISDN

- Placa de rede (NIC) conectada à rede interna.



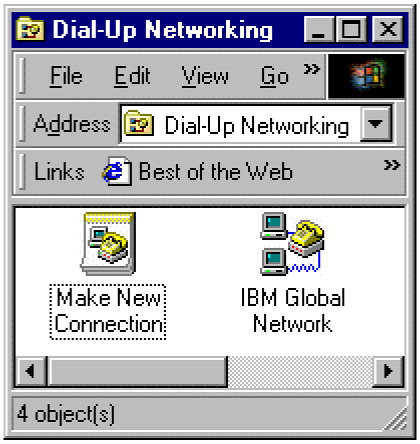
No caso de você ter um modem ISDN conectado ao seu computador por uma placa Ethernet, deve consultar o capítulo Conexão via DSL . Nesse caso você irá configurar o WinRoute para trabalhar com duas placas Ethernet.

Antes de conectar

Antes de conectar à Internet, verifique duas vezes o seguinte:

- · O protocolo TCP/IP está instalado e configurado corretamente (consulte a lista de verificação ou o capítulo Configurando a rede)
- · A rede dial-up (Windows 95/98) ou o serviço RAS (WindowsNT) está instalado e configurado corretamente
- · O modem está ligado ao PC host do WinRoute.

O WinRoute usa a rede dial-up ou o serviço RAS disponível em seu sistema operacional para a conexão à Internet.



Recomendamos que você estabeleça a conexão à Internet no computador onde o WinRoute será instalado ANTES de instalar e executar o WinRoute para garantir que a conexão está configurada corretamente e a rede dial-up ou o serviço RAS está funcionando sem problemas.

Configuração do WinRoute

Após ter efetuado toda a configuração descrita acima:

1 Vá ao menu Configurações->Tabela de interface - você deve poder ver todas as interfaces de rede disponíveis em seu computador. As interfaces discadas (dial-up) são nomeadas como RAS nos sistemas operacionais do WinRoute (no 95/98 e NT).

2 Vá às Propriedades da interface RAS selecionada

3 Marque a opção "Execute o NAT com o endereço IP desta interface em toda comunicação que passe por ela"

4 Vá à tabela RAS na caixa de diálogo Propriedades, escolha ou crie a sua conexão e configure as opções de acordo com as suas necessidades. Consulte a tabela RAS para maiores detalhes.

- ***Lembre-se! O NAT precisa estar ativo ("MARCADO") na interface RAS apesar de estar "DESMARCADO" na(s) interface(s) de conexão com a rede interna.***

Configuração da interface Ethernet

1 A placa ligada à rede interna tem um endereço IP atribuído (classe privativa) e NENHUM gateway atribuído!

2 As entradas do DNS usadas para esta interface são baseadas nos dados do seu provedor de acesso. Se estes dados não foram fornecidos a você, entre em contato com o seu provedor de acesso.

Você pode configurar o WinRoute para fornecer a você o recurso de discar sob demanda, onde a conexão é estabelecida automaticamente com base no tráfego (dados) de saída da rede local. Para maiores detalhes clique aqui.

Conexão pelo AOL

Usando o WinRoute Pro você pode conectar a sua rede à Internet via uma simples conta de acesso discado à AOL. Observação - A AOL suporta apenas computadores com Win95/98. Para conectar através da AOL siga os seguintes passos:

1 Instale o cliente AOL (preferivelmente o AOL 5.0 ou posterior)

2 Conecte à Internet para garantir que sua conexão não tem problemas

3 Instale o WinRoute Pro

4 Na administração do WinRoute vá ao menu *Configurações->Tabela de interface*

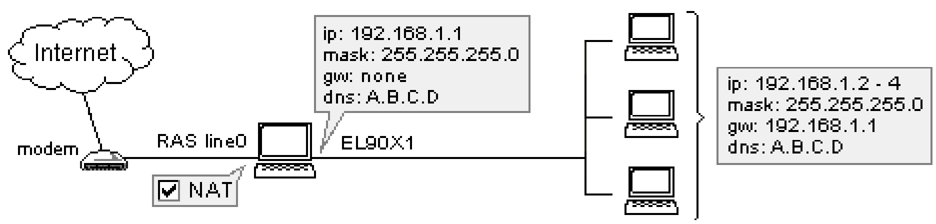
5 Você deve ver o adaptador AOL entre as interfaces disponíveis. Clique nas propriedades dessa interface e escolha "executar o NAT" na mesma interface.

Configure o seu computador do WinRoute e os computadores clientes de acordo com a lista de verificação (consulte outro capítulo).

➢ ***Observação! A discagem sob demanda não irá funcionar. Você precisa iniciar a conexão à AOL manualmente.***

Conexão T1 ou pela rede (LAN)

Conexões T1 ou via rede (LAN) exigem duas placas de rede (NIC) instaladas no computador do WinRoute. Uma placa servirá para a conexão com à Internet (p.ex. roteador) enquanto a outra servirá para a conexão com a rede interna.



Para conectar à Internet:

1 Vá ao menu Configurações->Tabela de interface

2 Escolha a placa de rede de conexão à Internet, clique em Propriedades e marque a opção "Execute o NAT com o endereço IP desta interface em toda comunicação que passe por ela". Ao abrir a caixa de diálogo da tabela de interface você verá o NAT ativo (ON) ao lado desta linha externa.

3 Certifique-se que o NAT NÃO está ativo (NOT ON) para a interface de conexão com a rede interna (vá às propriedades desta interface na tabela de interface)

4 Certifique-se de que NÃO há gateway definido nas propriedades do TCP/IP da placa de rede interna (vá às configurações da rede) e que há um endereço IP interno atribuído à placa.

5 Certifique-se de que a placa de rede de conexão à Internet foi configurada de maneira apropriada com os dados de seu provedor de acesso. No caso de você ter endereços IP atribuídos dinamicamente deixe as configurações de endereço IP em branco.

Para outras configurações de rede consulte os capítulos apropriados, especialmente a ***Lista de verificação*** .

Conexão pelo DirecPC

O DirecPC usa um modem (analógico, ISDN, ...) ou uma placa de rede (Ethernet, Token Ring) para o uplink enquanto usa uma antena parabólica de satélite para o download de dados. Sua conexão à Internet é fornecida pelo próprio DirecPC ou você pode usar a sua conexão por linha discada existente com o seu provedor.

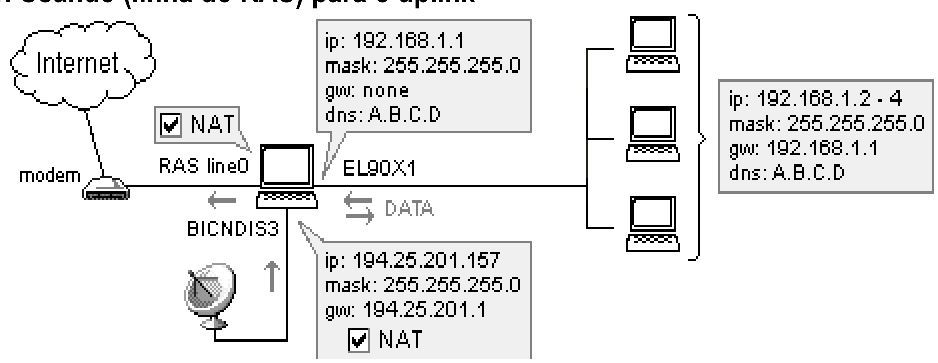
Os dados saem de seu computador via modem para o serviço Internet do DirecPC onde são roteados para o seu destino final. No caminho de volta o DirecPC associa os pacotes (dados) que vem para o seu computador com diferentes dados para roteá-los via antena parabólica de satélite.

Configuração do WinRoute

Em primeiro lugar você precisa ter todo o software e componentes do DirecPC instalados corretamente. Em seguida, prossiga com a configuração do WinRoute de acordo com as suas necessidades específicas.

Você pode escolher o discador do DirecPC ou o RAS do WinRoute para o uplink. Ao usar o WinRoute você terá o benefício do recurso de discagem sob demanda, isto irá economizar dinheiro em sua conta telefônica.

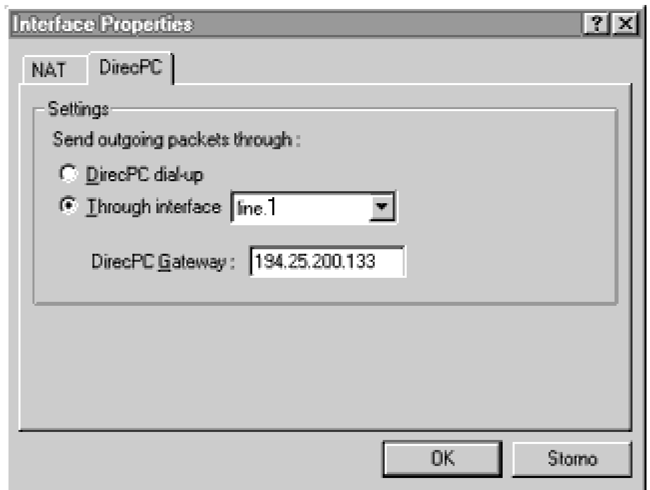
1. Usando (linha do RAS) para o uplink



Vá ao menu *Configurações->Tabela de interface*. Você verá a interface de linha do RAS (seu modem) e a placa de interface do DirecPC.

Clique na placa de interface do DirecPC e vá às "Propriedades". Você verá duas guias - **NAT** e **DirecPC**.

- Na guia NAT marque (ON) a opção *"Execute o NAT com o endereço IP desta interface em toda comunicação que passe por ela".*
- Na guia DirecPC escolha que você usará a *line0* para o uplink. Informe o *endereço IP do gateway* que foi fornecido a você pelo DirecPC.

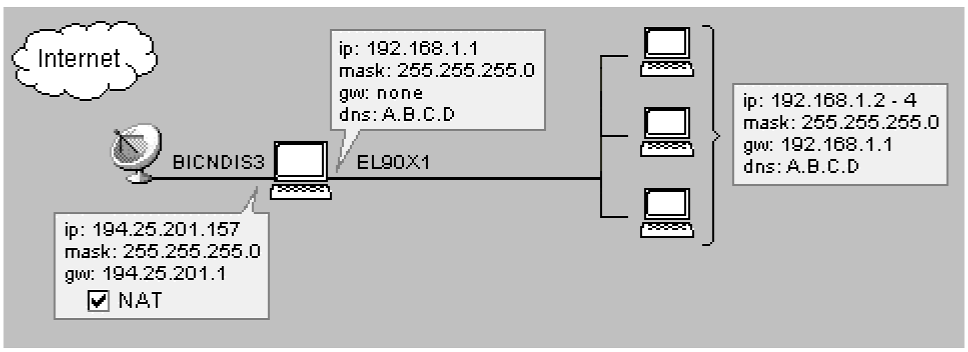


3. Clique na interface do RAS vá às "Propriedades". Marque (ON) a opção "Execute o NAT com o endereço IP desta interface em toda comunicação que passe por ela". Na guia RAS, selecione a conexão que você usará para o seu provedor de acesso, em seguida informe o seu nome de usuário e a senha.

➢ ***Observação! Você precisa DESMARCAR a opção "Use o gateway default na rede remota" nas propriedades da conta da rede dial-up criada para conectar com o provedor de acesso. Configure esta opção nas propriedades do TCP/IP de sua interface de conexão discada (dial-up).***

2. Usando o discador do DirecPC para o uplink

Você pode usar o discador embutido no DirecPC onde estiver disponível. De qualquer modo recomendamos o uso da linha do RAS do WinRoute onde for possível.



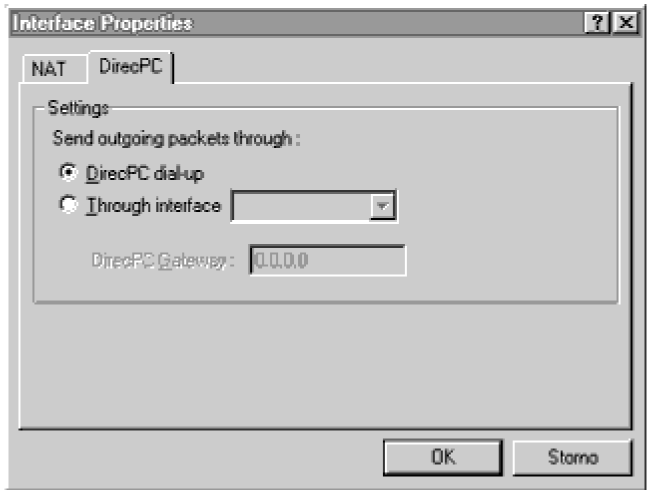
Para usar o discador do DirecPC:

Vá ao menu *Configurações->Tabela de interface*. Você verá a interface da linha do RAS (seu modem) e a placa de interface do DirecPC

Clique na placa de interface do DirecPC e vá às "*Propriedades*". Lá você verá duas guias - NAT e DirecPC.

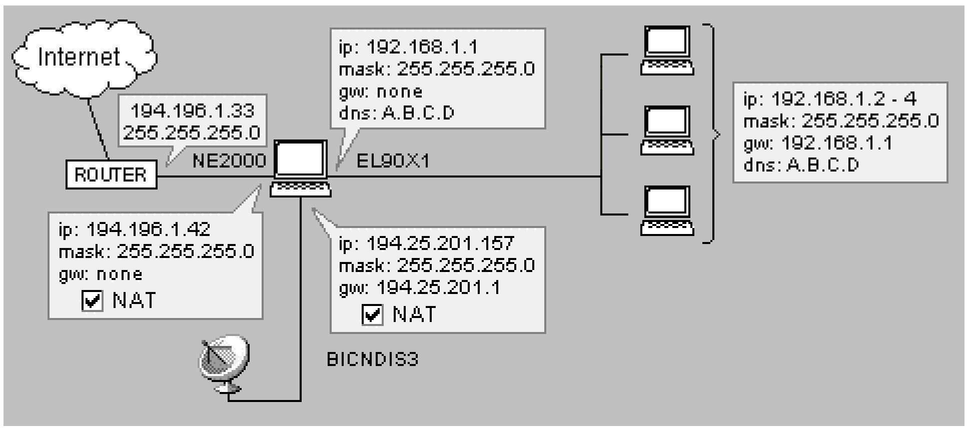
- Na guia NAT, marque (ON) a opção "*Execute o NAT com o endereço IP desta interface em toda comunicação que passe por ela*".

- Na guia DirecPC escolha "*Use o discador do DirecPC para o uplink*".

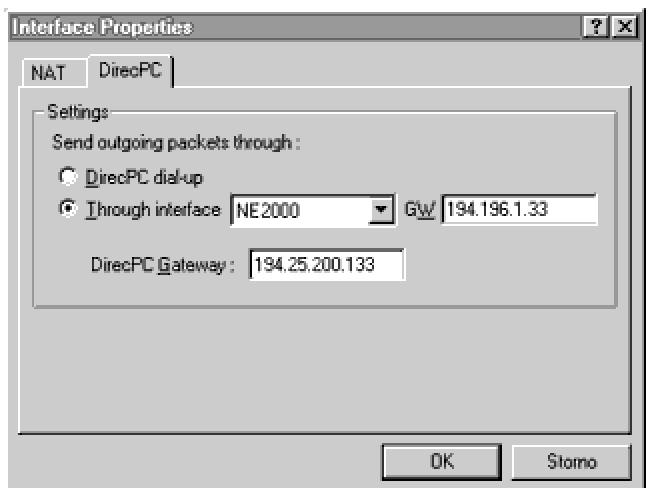


3. Usando a interface Ethernet para o uplink

Algumas vezes você pode querer usar a interface Ethernet para o uplink. Isto acontece normalmente se o uplink é realizado sobre uma conexão ISDN (e você tem um roteador ou modem ISDN) ou V-SAT (parabólica com adaptador Ethernet).



Vá à caixa de diálogo de propriedades da placa de interface do DirecPC.



- Na guia NAT, marque (ON) a opção "*Execute o NAT com o endereço IP desta interface em toda comunicação que passe por ela*".
- Na guia DirecPC escolha "*Através da interface*" e selecione a interface com conexão à Internet. Em seguida, informa o gateway default de seu provedor de acesso no campo "GW" (p.ex. 194.196.1.33).

Aumentando o throughput

Para obter o maior throughput de dados possível durante uma conexão à Internet com o uso do DirecPC, reduza a **janela de recepção do TCP** em todos os computadores que usarão o DirecPC:

No Windows NT:

1. Vá à entrada de registro HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
2. Adicione uma entrada (se já existir, edite-a) chamada "TcpWindowSize" (é do tipo DWORD) no registro. Configure seu valor para 0xBB80.

No Windows 95:

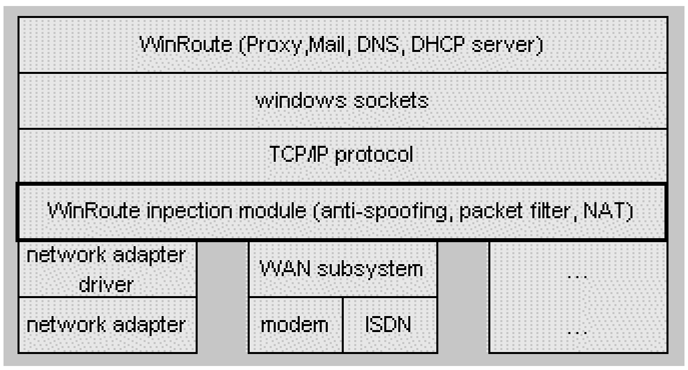
1. Vá à entrada de registro HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\VxD\MSTCP.
2. Adicione uma entrada (se já existir, edite-a) chamada "DefaultRcvWindow" (é do tipo string) no registro. Configure seu valor para "0xBB80".

Configurando a segurança

Nesta seção

Segurança do NAT

O WinRoute efetua as operações do NAT na mais baixa camada de protocolo de rede possível. O WinRoute controla o tráfego entre o driver da placa de rede (NIC, network interface card) e a pilha do TCP. O WinRoute tem o controle mais atual sobre o tráfego de Internet, capturando os pacotes de saída e de entrada, o que minimiza as chances de ser interrompido. Este é um recurso único da implementação do NAT do WinRoute. E isto também provê melhorias de segurança adicional tais como o firewall ou anti-spoofing baseado na filtragem de pacotes. Com o NAT do WinRoute a rede inteira está totalmente protegida, incluindo o computador com o WinRoute.



Opções de segurança do NAT

Nas configurações avançadas do WinRoute (build 20 e posteriores) há um menu de opções de segurança do NAT que incorpora um **modo silencioso**. **Modo silencioso** significa que, para tipos específicos de solicitações, o WinRoute pode "derrubar" pacotes de forma que sua rede mostre-se invisível para o mundo externo.

Solicitação de eco do ICMP de entrada:

O Internet Control Message Protocol (ICMP) é o protocolo unicamente para envio de uma solicitação de informações (pingar, exemplo - ping 206.86.211.32). Quando qualquer computador tenta **pingar** o host do WinRoute, as **Opções de segurança do NAT** oferecem duas reações:

- Se você selecionar a opção *"enviar resposta a eco do ICMP"* o computador solicitante receberá a resposta.
- Se você selecionar a opção *"derrubar solicitação (modo silencioso)" o datagrama será derrubado*, simplesmente perdido em trânsito. Em seguida, a ponta solicitante receberá a mensagem *"host de destino inacessível."*

Pacotes de entrada sem entrada na tabela do NAT:

O WinRoute inspeciona todo o tráfego de entrada e de saída de uma rede. Se o WinRoute está para executar ou não o NAT em um determinado pacote, primeiramente ele examinará o pacote e registrará certas informações tais como o número da porta e o endereço IP na tabela do NAT. Desta maneira, quando da volta do pacote de retorno, o WinRoute pode compará-lo com a tabela NAT para determinar para quem rotear o pacote de volta. Se o pacote não está iniciado, significando que não é um pacote de retorno, o WinRoute irá compará-lo com a tabela do NAT e determinar que o mesmo não está iniciado. Se nenhum mapeamento de porta foi criado, o WinRoute não estará apto a enviar o pacote para qualquer um por dentro da rede.

- A opção "enviar pacote de negação" simplesmente retornará um pacote ao emitente informando que a conexão não pode ser estabelecida.

- A opção “derrubar pacote (modo silencioso)" eliminará o pacote e não enviará um pacote de retorno. Desta maneira o host do WinRoute, assim como a rede por trás dele, parecerá que não existe.

Nos pacotes UDP de entrada:

Algumas aplicações que usam o **User Datagram Protocol** (UDP) exigem que você envie pacotes UDP para um servidor central. O WinRoute registra a origem e o destino de todos os pacotes UDP de saída para o servidor atribuído pela aplicação que envia o pacote. Em alguns casos, o servidor pode passar seu endereço IP e a porta para um outro computador que em seguida envia a você um pacote UDP com a informação que você solicitou. Mesmo que este computador aleatório tenha um endereço IP diferente do servidor, ainda pode enviar pacotes UDP para dentro de sua rede porque ele sabe qual o endereço IP e qual porta usar.

- Usando este exemplo, se você selecionar “*pode passar pelo NAT com qualquer endereço IP de origem*” o pacote UDP passará através do WinRoute.
- Para melhorar a segurança, você pode selecionar “*pode passar pelo NAT apenas se vier do endereço IP de origem registrado quando o primeiro pacote de saída da rede foi enviado.*” Isto pode permitir que apenas os pacotes UDP do servidor central passem através do WinRoute.

Opções de log do NAT:

Dentro das opções avançadas de segurança há a habilidade de registrar informações de pacotes que entram na rede e que não foram originalmente solicitados por qualquer um de dentro da rede. Isto normalmente faz parte de redes nas quais funcionam servidores Web, FTP, DNS ou de outros tipos por trás do WinRoute e isto é muito útil na determinação da origem de um problema.

Log de pacotes de chegada sem entrada na tabela do NAT:

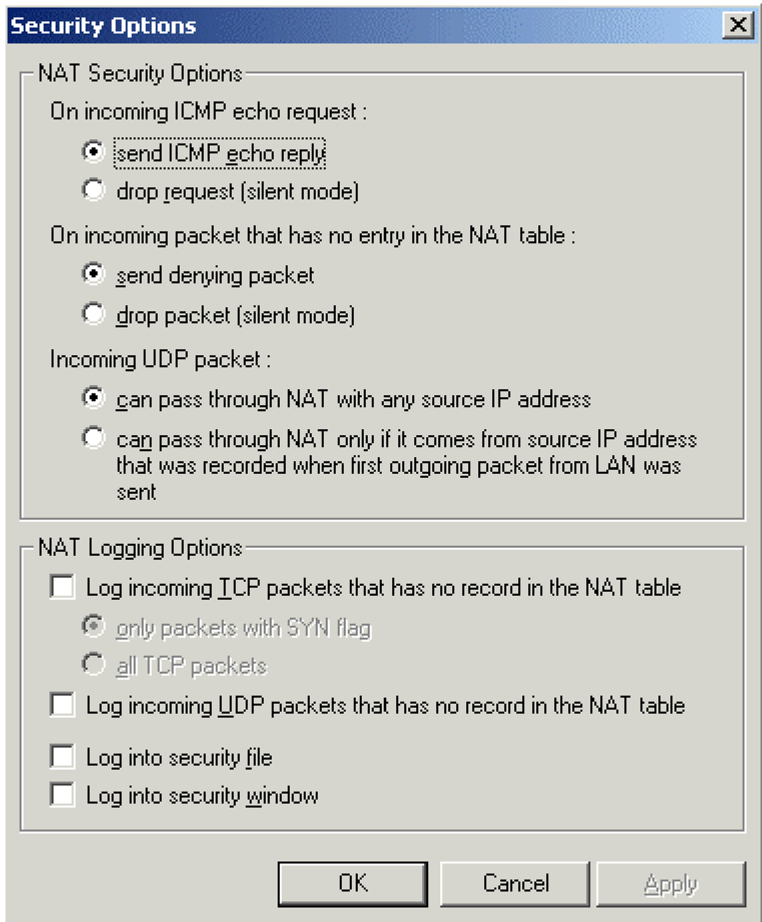
O WinRoute oferece duas opções de registrar o log de pacotes TCP que não estão na tabela do NAT.

- Se você escolher registrar o log "*apenas de pacotes com o sinalizador SYN*" (sincronizar), o pacote TCP será registrado no log apenas se uma conexão foi estabelecida entre o remetente e o receptor.

- A opção "*todos os pacotes TCP*" simplesmente registra no logo todos os pacotes TCP de entrada não importando se uma conexão foi estabelecida ou não. Uma vez que os pacotes UDP não usam sinalizadores, todos os pacotes UDP que não estão iniciados serão registrados no log se você escolher registrá-los.

Log em um arquivo ou janela:

- Se você selecionar "*registrar o log dentro da janela de segurança*" pode escolher por visualizar as informações do log da aplicação de administração do WinRoute pelo menu Exibir-Registros de Log-Log de segurança.
- Se você escolher "*registrar o log em um arquivo*", o WinRoute gravará as informações no log de segurança, na pasta de logs do WinRoute Pro (normalmente c:/Program Files/WinRoute Pro/Logs)


Security Options
NAT Security Options
On incoming ICMP echo request :
send ICMP echo reply
drop request (silent mode)
On incoming packet that has no entry in the NAT table :
send denying packet
drop packet (silent mode)
Incoming UDP packet :
can pass through NAT with any source IP address
can pass through NAT only if it comes from source IP address that was recorded when first outgoing packet from LAN was sent
NAT Logging Options
Log incoming TCP packets that has no record in the NAT table
only packets with SYN flag
all TCP packets
Log incoming UDP packets that has no record in the NAT table
Log into security file
Log into security window
OK
Cancel
Apply

Configurações de filtragem de pacote

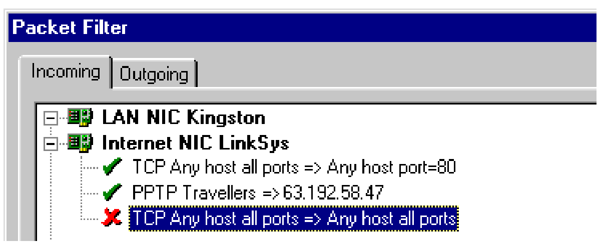
A configuração da porção de filtragem de pacote do firewall do WinRoute Pro é muito simples. Porém, exige um bom entendimento da lógica por trás da funcionalidade de filtragem de pacotes aplicada no WinRoute.

Conjunto de regras por interface

Os usuários podem definir regras de segurança separadas para interfaces individuais de computador que você tenha em sua máquina. Isto é um recurso muito importante na administração de redes de múltiplos segmentos.

Exempla: a imagem a seguir mostra o exemplo de rede que:

- *permite que qualquer um da Internet tenha acesso ao servidor Web dentro de sua rede*
- *permite apenas que determinados indivíduos do grupo de endereços predefinido chamado Travellers tenham acesso ao servidor PPTP dentro da rede para poder entrar na rede*

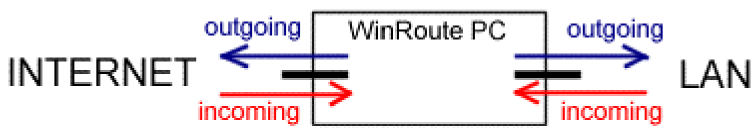


Regras separadas para pacotes de saída e de entrada

O WinRoute aplica regras específicas para pacotes de saída e pacotes de entrada. Uma tabela é criada dentro do WinRoute para cada interface. Os pacotes de entrada e os pacotes de saída são registrados nesta tabela. Em outras palavras, cada pacote tem duas entradas, uma para saída e outra para entrada.

O que é um pacote de SAÍDA/ENTRADA?

O WinRoute sempre considera o seu "motor" (engine) como a peça de centro do sistema inteiro. Isto significa que todos os pacotes que deixam o WinRoute são de SAÍDA não importando de eles vão para a Internet ou para a rede local. De maneira similar os pacotes que chegam AO PC do WinRoute PC são de ENTRADA não importando de onde vêm. Considere isto ao criar as suas regras de segurança.



APLICAÇÃO DE REGRAS:

De CIMA pata BAIXO

As regras estão definidas em uma lista e são aplicadas de cima para baixo. Após a chegada do pacote na interface, este é verificado junto à lista de critérios definidos. O exame começa pelos critérios no topo da lista e continua até a parte mais inferior da mesma. Quando o pacote atende aos critérios, a regra é aplicada e as regras restantes são omitidas.

As regras podem ser aplicadas a:

- usuários independentes
- faixa de endereços IP
- um grupo de endereços IP definido pelo usuário (para definir um grupo de usuários consulte a parte de referência deste manual)

- sub-rede ou a rede inteira



As regras podem ser aplicadas em uma zona de tempo predefinida

Em alguns casos, isto pode ser útil para aplicar regras específicas durante o horário comercial e critérios diferentes para o acesso fora desse horário. Ou, você pode desejar permitir que certos usuários tenham acesso à Web durante o horário de almoço e, durante o horário de trabalho, limitar o acesso apenas a determinados recursos.

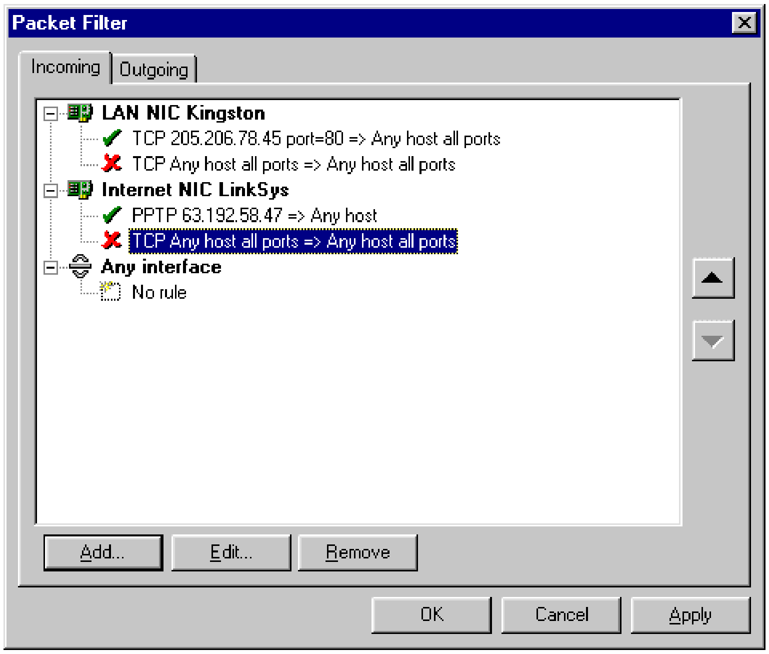
Exemplo:

Controle total de acesso do usuário: O administrador da rede deseja que apenas os usuários autorizados tenham acesso à sua rede, para que tenham permissão para entrar. No entanto, muitas configurações de rede têm servidores da Web e de FTP por trás do sistema do WinRoute e que precisam de acesso público.

No caso acima, as regras poderiam ser definidas na seguinte ordem para os pacotes de entrada:

1. Aceitar pacotes de qualquer host que se dirijam para a porta 80
2. Aceitar pacotes de qualquer host que se dirijam para a porta 21
3. Recusar todos os pacotes

Se o pacote de entrada se adequar à regra 1 ou 2 é permitido que passe e a regra 3 não é aplicada. Se ele não se adequar à regra 1 ou 2, então é recusado.



Conjunto de regras simples para filtragem de pacote básica

Regras de entrada (certifique-se que elas estejam nesta ordem)

Protocolo	Origem	Destino	Tipos de ICMP	Ação	Log	
UDP	Qualquer endereço, porta = 53	Qualquer endereço, porta > 1023		Permitir		
TCP	Qualquer endereço, qualquer porta	Qualquer endereço, porta > 1023		Permitir TCP verificado		
ICMP	Qualquer endereço	Qualquer endereço	Resposta ao eco	Permitir		
IP	Qualquer endereço	Qualquer endereço		Derrubar	Na janela	

Observação: Esta última "regra de limpeza" irá interferir com quaisquer ferramentas de captura de pacotes de rede usadas neste host.

Conjunto de regras simples para filtragem de pacote básica de HTTP e FTP de entrada

Protocolo	Origem	Destino	Tipos de ICMP	Ação	Log	De
TCP	Qualquer endereço, qualquer porta	[este host], porta = 80		Permitir	(opcional)	Per (se par
TCP	Qualquer endereço, qualquer porta	[este host], porta = 21		Permitir	(opcional)	Per FT
TCP	Qualquer endereço, qualquer porta	[este host], porta = 20		Permitir	(opcional)	Per FT (ap pas tod nãc

Permitindo a comunicação em certas portas

Você quer aplicar as seguintes regras:

- segurança máxima
- permitir acesso ao seu servidor da Web
- permitir comunicação com o seu servidor SMTP

- permitir a recepção de e-mail da Internet no seu servidor de correio
- permitir acesso ao seu servidor de FTP

Segurança máxima:

Guia Entrada

Protocolo: TCP, recusar todos os pacotes de entrada

IP de origem - qualquer	IP de destino - qualquer
Porta de origem - qualquer	Porta de destino - qualquer

Esta regra sempre será a última das regras disponíveis na interface.

Permitir acesso da Internet ao seu servidor da Web:

Guia Entrada

Protocolo: TCP

IP de origem - qualquer	IP de destino - endereço IP do servidor da Web
Porta de origem - qualquer	Porta de destino - 80

Permitir acesso a partir de certos endereços da Internet ao seu servidor de FTP:

Guia Entrada

Protocolo: TCP

IP de origem - qualquer	IP de destino - endereço IP do servidor de FTP
Porta de origem - qualquer	Porta de destino - 21

IP de origem - qualquer	IP de destino - endereço IP do servidor de FTP
Porta de origem - qualquer	Porta de destino - 20

Permitir que o seu servidor SMTP se comunique apenas por meio de seu servidor SMTP de retransmissão (no provedor de acesso):

Guia Entrada

Protocolo: TCP

IP de origem - servidor SMTP de retransmissão do provedor de acesso	IP de destino - endereço IP do servidor SMTP em sua rede local
Porta de origem - qualquer	Porta de destino - 25

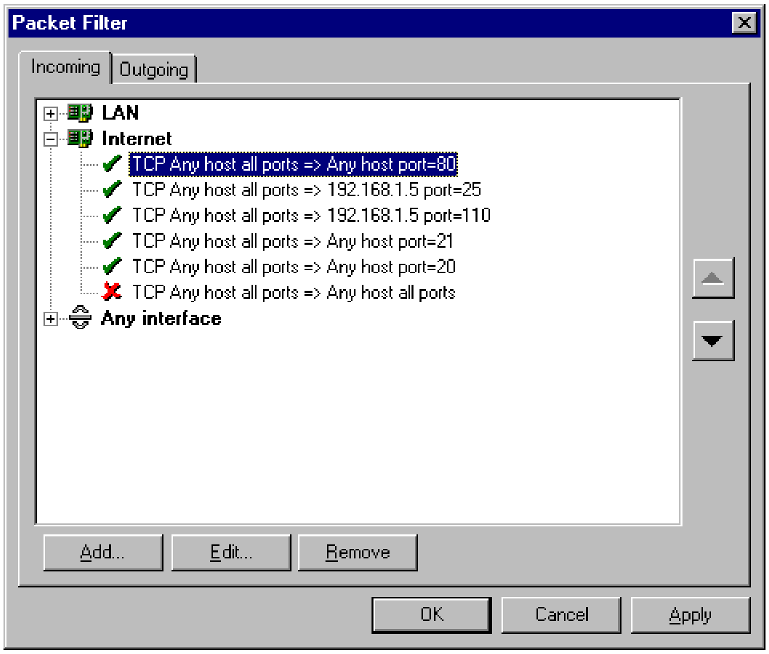
Guia Saída

IP de origem - seu servidor SMTP	IP de destino - endereço IP do servidor SMTP no provedor de acesso
Porta de origem - qualquer	Porta de destino - 25

Permitir que você receba e-mail da Internet no seu servidor de correio:

Guia Entrada

IP de origem - seu servidor SMTP	IP de destino - endereço IP do servidor SMTP em sua rede local
Porta de origem - qualquer	Porta de destino - 110


Packet Filter
Incoming
Outgoing
LAN
Internet
TCP Any host all ports => Any host port=80
TCP Any host all ports => 192.168.1.5 port=25
TCP Any host all ports => 192.168.1.5 port=110
TCP Any host all ports => Any host port=21
TCP Any host all ports => Any host port=20
TCP Any host all ports => Any host all ports
Any interface
Add...
Edit...
Remove
OK
Cancel
Apply

Obrigando usuários a usarem o servidor proxy

Algumas vezes você pode achar útil usar o **servidor proxy** embutido no WinRoute. É de grande utilidade quando você quer **monitorar** a atividade de usuários em seu acesso à páginas da Web ou se você quer **aplicar restrições** a clientes no acesso a certos sites da Web ou quando você quer que eles usem o **cache**.

➢ ***Observação! Você pode usar a filtragem de pacotes para controlar o tráfego da Web; no entanto, é mais fácil com o uso do*** *filtro embutido de URL do proxy* ***porque ele resolve nomes de domínio, permitindo que você apenas tenha que informar a URL ao invés do endereço IP associado.***

Configurações:

Você tem que criar duas regras de segurança para os pacotes de **saída**:

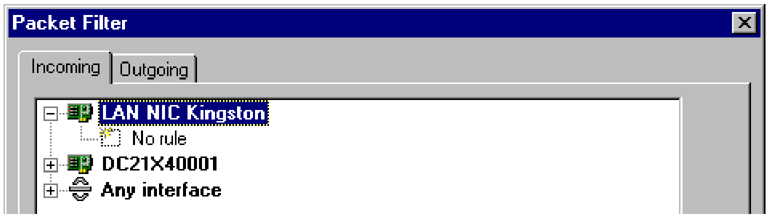
1. **Permitir** que pacotes de saída com *porta de destino 80 e endereço IP de origem* de qualquer host do WinRoute
2. **Negar** todos os pacotes de saída com *porta de destino 80*

As regras precisam ser aplicadas exatamente na ordem descrita acima. O WinRoute aplica as regras na ordem de **cima-para-baixo**. As regras são aplicadas em uma base "primeiro a chegar, primeiro a ser servido", isto é, o pacote de entrada é confrontado com as regras onde a regra do topo da lista é a primeira e a regra da base da lista é a última. A primeira regra que se encaixe à descrição do pacote é aplicada enquanto o restante das regras é omitido.

Para configurar regras:

1. Na administração do WinRoute vá ao menu *Configurações=>Avançadas=>Filtro de pacotes*. Vá à guia *Saída*.

2. Dê um clique duplo na sua interface externa (Internet). Será exibida a lista de regras ou a mensagem "Sem regra".



3. Pressione o botão *Adicionar* para adicionar uma nova regra que habilitará o host do WinRoute a estabelecer conexões com servidores da Web na porta 80.

Protocolo selecionado: TCP

Tipo de origem: Host

Endereço IP: endereço externo do seu Firewall do WinRoute (p.ex. 204.23.43.26)

Porta de destino: igual a (=) 80, em Ação: selecione Permitir.

4. Pressione o botão *Adicionar* novamente para adicionar uma segunda regra que irá recusar todas as outras conexões TCP para a porta 80.

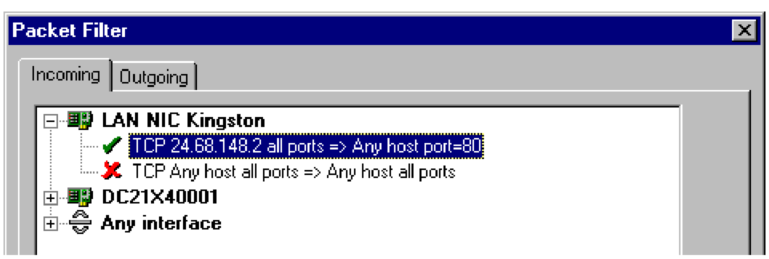
Protocolo selecionado: TCP

Tipo de origem: qualquer

Porta de destino: igual a (=) 80

Ação: Recusar.

Se você quiser registrar no log as tentativas, marque a caixa de seleção Log em arquivo.



- ***OBSERVAÇÃO: Ao configurar regras adicionais, lembre-se de criar regras de CIMA para BAIXO.***

Configurando o servidor de correio

Nesta seção

Usuários de correio

Existem várias regras básicas sobre usuários, endereços de e-mail e caixas de correio no WinRoute.

Um usuário = uma caixa de correio...

Cada usuário do WinRoute tem uma **caixa de correio** criada para ele. A caixa de correio tem o nome do usuário. No case do você ter um domínio registrado na Internet e informado no WinRoute, o endereço de e-mail do usuário será automaticamente usuário@domínio.com.

Um usuário = mais endereços

Para usar endereços de e-mail diferentes e criar várias caixas de correio como vendas@..., suporte@...., info@... você deve definir aliases. As combinações são praticamente infinitas.

Para adicionar usuários:

1. Vá ao menu **Configurações=>Contas**
2. Adicione **usuários**
3. Agrupe usuários em **grupos** se necessário

Exemplo:

A empresa tem o domínio brutus.com. O usuário John terá um endereço de e-mail igual a john@brutus.com. Para outras opções de endereçamento consulte Aliases.

- ***Observação: As caixas de correio são mantidas em um diretório separado. Normalmente em c:/Program files/WinRoute/Mail. As caixas de correio são fisicamente criadas APÓS a chegada do primeiro.***

Enviando e-mail para os outros usuários do WinRoute dentro de sua rede

Para enviar um e-mail para outros usuários **dentro** de sua rede local use o **nome de usuário do WinRoute** do destinatário ao invés do endereço de **e-mail (Internet)**.

Exemplo: O nome de usuário do destinatário é John e seu endereço de e-mail completo é john@company.com. Você pode informar apenas *john* no campo *Para:* da mensagem de e-mail.

Questão com aliases

Se você usa o **endereço completo de e--mail** de um usuário local a mensagem será enviada **através** da Internet, isto é, para o servidor SMTP de retransmissão e, em seguida, de volta para o WinRoute. Para impedir que isso ocorra você precisa especificar aliases.

- ***Lembre-se! Você precisa configurar o PC do WinRoute como o seu servidor de correio de saída (SMTP).***

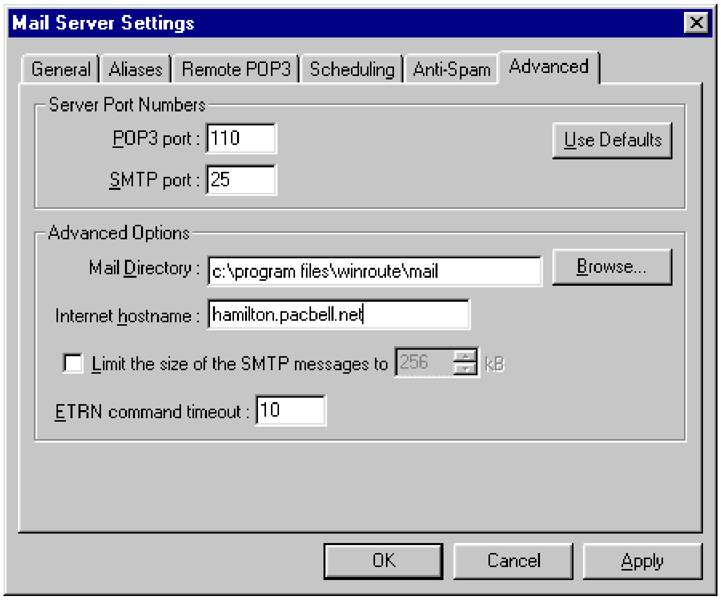
Questão da autenticação

Autenticação

Alguns provedores de acesso fazem a autenticação do e-mail que passa por eles para impedir a ocorrência de spam. Então você tem que fornecer informações suficientes ao seu provedor de acesso.

1. Vá até a janela da guia *Servidor de correio->Avançado*

2. Informe o **nome do host** desejado no campo nome do host Internet. Normalmente este é o nome do computador conectado à Internet, p.ex. *host.isp.com*.



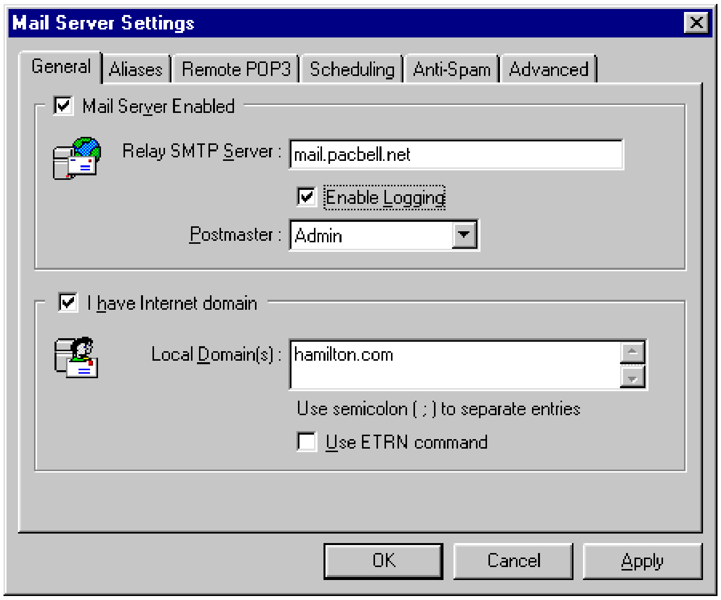
Enviando e-mail para a Internet

Você pode usar o WinRoute como o seu **servidor SMTP** para as mensagens de saída. O WinRoute usa o **servidor SMTP de retransmissão** do seu provedor de acesso para enviar e-mail ao invés de usar registros MX. Em outras palavras - todo o e-mail de saída será enviado pelo outro servidor de correio que você informar (normalmente o servidor de correio do seu provedor de acesso). As mesmas regras podem ser aplicadas aos seus clientes de e-mail - o servidor de correio do WinRoute pode ser o servidor SMTP de retransmissão deles.

Para definir o servidor de SMTP de retransmissão para correio de saída:

1 Vá ao menu *Configurações=>Servidor de correio*

2 Informe o servidor de correio de saída de seu provedor de acesso no campo *Servidor SMTP de retransmissão*

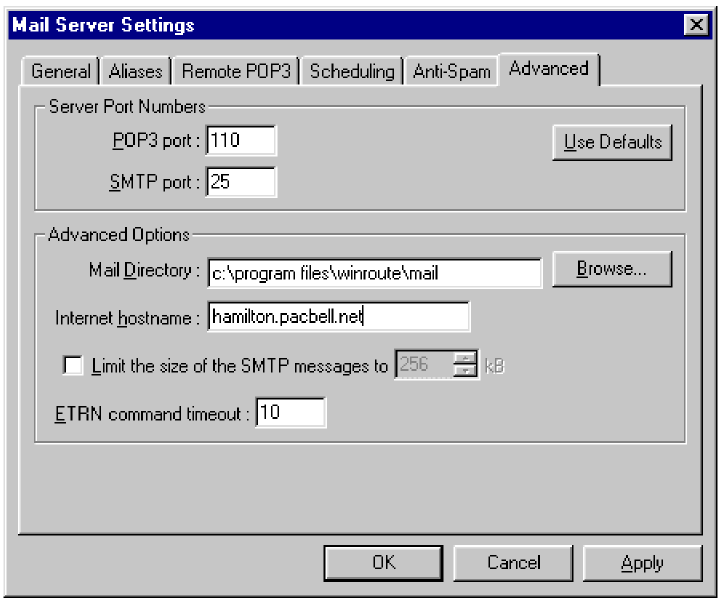


Autenticação

Alguns provedores de acesso fazem a autenticação do e-mail que passa por eles para impedir a ocorrência de spam. Então você tem que fornecer informações suficientes ao seu provedor de acesso.

1. Vá até a janela da guia *Servidor de correio->Avançado*

2. Informe o **nome do host** desejado no campo nome do host Internet. Normalmente este é o nome do computador conectado à Internet, p.ex. *host.isp.com*.



Aliases

Os **aliases** são usados no WinRoute para endereços **adicionais** dos usuários e também para **substituição** de endereço de e-mail.

Com os **aliases** você pode:

- atribuir mais endereços a um usuário
- atribuir um endereço de e-mail a mais de um usuário
- atribuir um endereço de e-mail a um grupo de usuários
- atribuir endereços a grupos

Exemplo:

Este exemplo mostra que as possibilidades são praticamente infinitas.

A empresa tem dois domínios:

- company.com
- company2.com

O usuário *John* pode receber e-mail por:

john_speaker@company.com

john@company2.com

sales@company.com

support@company.com

O e-mail enviado para *sales@company.com* poderia ser entregue ao grupo *[Sales]*.

Solução:

1. Vá à guia *Configurações=>Servidor de correio=>Aliases*.

2. Adicione os seguintes aliases:

*john** entregar para *John* -

isto entregaria todo o e-mail vindo da Internet no qual john aparece como o destinatário. Isto é, *john_speaker@company.com* assim como *john@company2.com* seriam entregues a um usuário *John.* Isto também evita que mensagens enviadas por usuários locais para o endereço *john@company.com* trafeguem pela Internet e o e-mail será entregue diretamente à caixa de correio do John no WinRoute.

sales entregar para *John* -

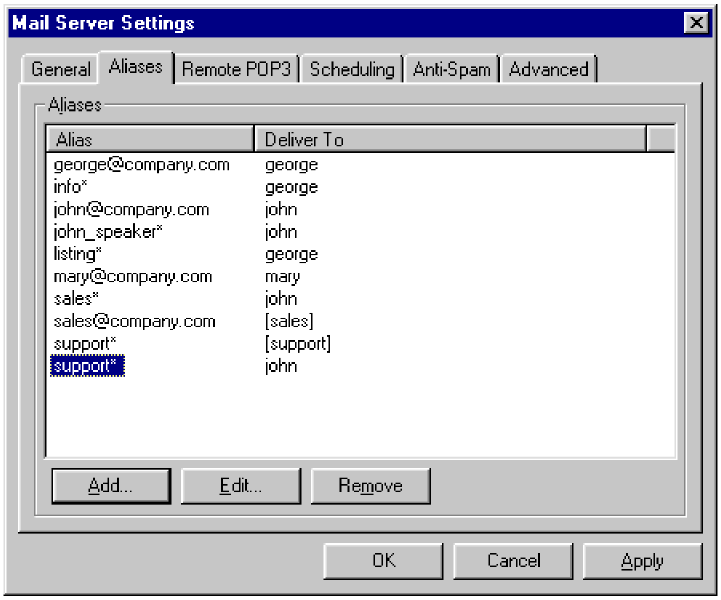
isto entregará todas as mensagens destinadas a *sales@……..* para um usuário *John*

Support entregar para *John* -

isto entregará todas as mensagens destinadas a *support@……* para *John*

Sales entregar para *[Sales]* -

isto entregará todas as mensagens destinadas a *sales@….* para todos os membros do *[Sales]*



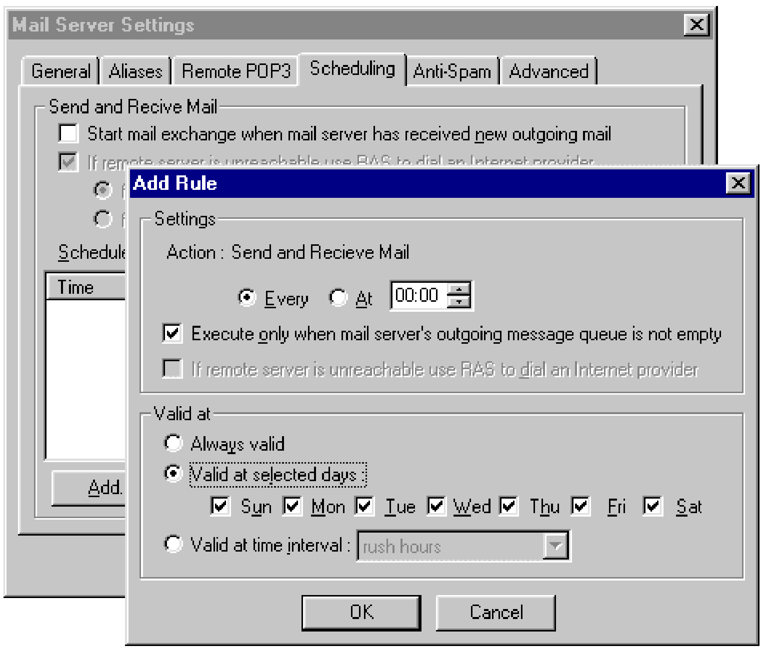
Agendando a troca de mensagens

O agendamento nas configurações do servidor de correio dá a você a opção de definir:

- intervalos regulares para a verificação de chegada de e-mail em seu provedor de acesso (seja POP3 ou SMTP usando ETRN)
- regras para o envio de e-mail
- os intervalos de tempo nos quais as regras são válidas. Você pode predefinir os intervalos de tempo no menu *Configurações->Avançadas->Intervalos de tempo*

Você pode decidir por enviar uma nova mensagem (e-mail) imediatamente após a chegada da mesma ao servidor de correio ou apenas em um período predefinido de tempo.

Você também pode selecionar se o servidor de correio discará ou não automaticamente no caso de haver nova mensagem. Se você selecionar esta opção, o servidor de correio do WinRoute estabelecerá a conexão toda a vez em que um dos seus usuários for enviar um novo e-mail.



Para receber e-mail você deve especificar o calendário inteiro informando exatamente quando gostaria de receber o correio. Você pode combinar diferentes regras para fazer a recepção de e-mail tão efetiva quanto possível.

1 Vá ao menu *Configurações->Servidor de correio->Agendamento*

2 Especifique as opções de sua escolha e adicione novas regras para a verificação de e-mail.

➢ ***Observação! As regras de "intervalos de tempo" devem ser definidas no menu Configurações->Avançadas->Intervalos de tempo***

Recebendo e-mail

Nesta seção

Você tem um domínio (SMTP)

O servidor de correio do WinRoute é totalmente compatível com ***SMTP***[1] e ***POP3***[2]. Você pode ter registrado o seu **domínio Internet** e receber e-mail via SMTP e/ou o WinRoute pode receber automaticamente receber o e-mail da conta POP3 do seu provedor de acesso.

---

[1] O **SMTP** (Simple Mail Transfer Protocol) é usado na comunicação direta entre servidores de correio (tal como o servidor de correio do WinRoute e o servidor de correio do seu provedor de acesso) e para o envio de mensagens a partir do seu software cliente de e-mail. O SMTP é um protocolo de "uma via" - isto é, as mensagens podem ser enviadas ou recebidas pelo servidor de correio mas não é possível recolher as mensagens em qualquer outro servidor de correio com o uso deste protocolo.

O protocolo SMTP é um protocolo TCP que opera na **porta 25**. Se você quiser ter acesso a este protocolo com servidor de correio em execução por trás no computador do WinRoute (para permitir a outro servidor de correio que envie as suas mensagens ou para usar este servidor de correio para as suas mensagens de saída se você está em sua rede local) você tem que efetuar um **mapeamento de porta** do protocolo TCP, porta 25 enviado para um endereço IP de **classe privativa** do PC em que o servidor de correio está sendo executado.

[2] O protocolo **POP3** é usado principalmente por software cliente de e-mail para pegar as mensagens nas caixas de correio em um servidor de correio compatível com o POP3. O servidor de correio do WinRoute tem tal capacidade também, isto é, pode pegar as mensagens automaticamente em qualquer servidor de correio compatível com POP3 e posteriormente distribui-las para as caixas de correio dos destinatários locais.

O protocolo POP3 é um protocolo **TCP** que funciona na **porta 110**. Se você quiser ter acesso a este servidor de correio em execução por trás do WinRoute ou no computador onde o WinRoute está instalado (para pegar s suas mensagens DA Internet) você tem que efetuar o **mapeamento de porta** do protocolo TCP, porta 110 enviado para o endereço IP de **classe privativa** do PC em que o servidor de correio está sendo executado.

Se você tem um domínio Internet registrado no seu endereço IP externo (público) o WinRoute pode receber e-mail pelo protocolo SMTP. Na guia Geral, da caixa de diálogo Servidor de correio, insira o nome do domínio registrado.

➢ ***Não se esqueça de mapear a porta 25 do protocolo TCP para o endereço IP de classe privativa da sua caixa no WinRoute! Do contrário o protocolo SMTP não terá permissão de passar pelo NAT do WinRoute!***

Com base em sua conexão à Internet você pode considerar o seguinte:

1 Você tem uma conexão permanente

Nenhuma configuração específica é necessária. Apenas o(s) domínio(s) informado(s)

2 Você tem uma conexão discada ou ISDN (comando ETRN)

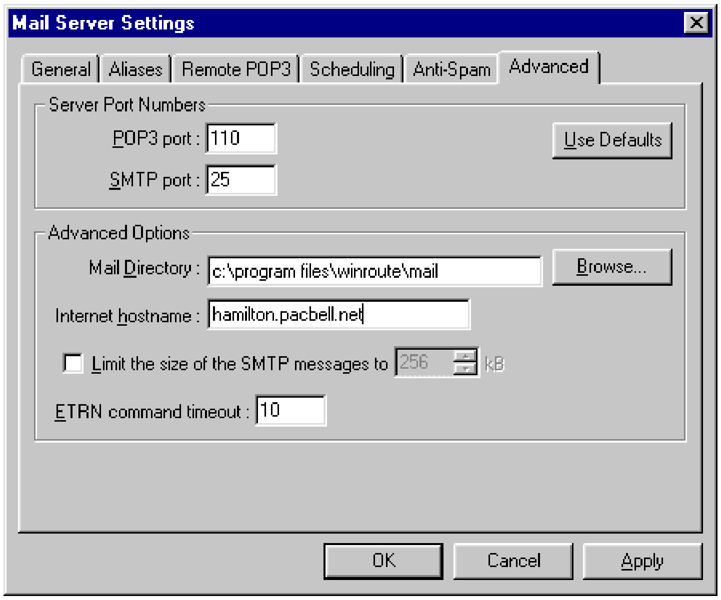
No caso de você não estar permanentemente conectado o seu e-mail é armazenado temporariamente no provedor de acesso. Em seguida este e-mail é transferido quando você se conecta. Alguns provedores de acesso exigem o uso de comando ***ETRN***[3] para procurar por novo e-mail. O servidor de correio do WinRoute suporta o comando ETRN. Você pode marcar esta opção na guia *Gera*l da caixa de diálogo do **Servidor de correi**o.



[3] O ETRN é um comando usado pelos servidores SMTP para negociar uma maior tempo, após o estabelecimento de uma conexão o servidor SMTP pode fazer uma consulta por correio SMTP.

O comando ETRN é sempre usado onde um servidor SMTP não está "online" 24 horas e o e-mail de tal servidor SMTP precisa ser armazenado temporariamente em outro servidor SMTP.

Se for necessário, você pode configurar o tempo ou intervalo do ETRN (vá à guia *Avançado*).



Tempo limite do comando ETRN

Esta entrada especifica quanto tempo após o estabelecimento de uma conexão, o servidor SMTP do poderá procurar por correio SMTP.

Múltiplos domínios

Múltiplos domínios

Você pode ter diversos domínios atribuídos à sua conexão à Internet. Se for o caso informe-os todos na guia *Configurações=>Servidor de correio=>Geral* e separe-os por ponto e vírgula.



Questões com múltiplos domínios

Existem duas maneiras de organizar múltiplos domínios atribuídos à sua rede:

1 Cada domínio está associado com o seu próprio endereço IP

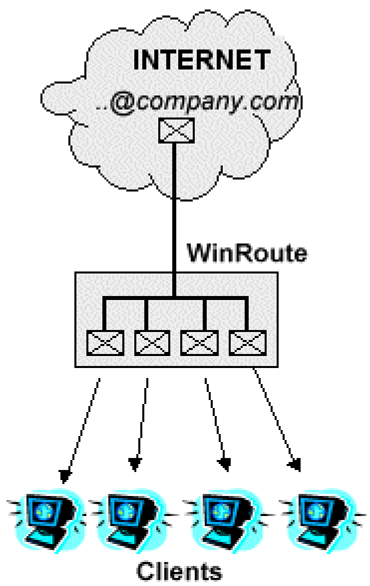
Nesta situação você tem que ter mais endereços IP públicos mapeados para a interface usada pelo WinRoute para as conexões à Internet. Em seguida você deve usar mais configurações de mapeamento de porta - uma para cada endereço IP - com o mesmo endereço IP de destino do computador do WinRoute.

2 Todos os domínios estão associados com um endereço IP

Não há a necessidade de configurações especiais além de configurar o mapeamento de porta do protocolo TCP na porta 25 para o endereço IP local de seu computador do WinRoute.

Você tem um domínio atribuído a uma conta POP3

Você pode combinar com o seu provedor de acess de que todo o e-mail para o seu domínio vá para uma única conta. O WinRoute pode verificar essa conta, pegar as mensagens e distribuí-las automaticamente para as caixas de correio dos usuários locais.

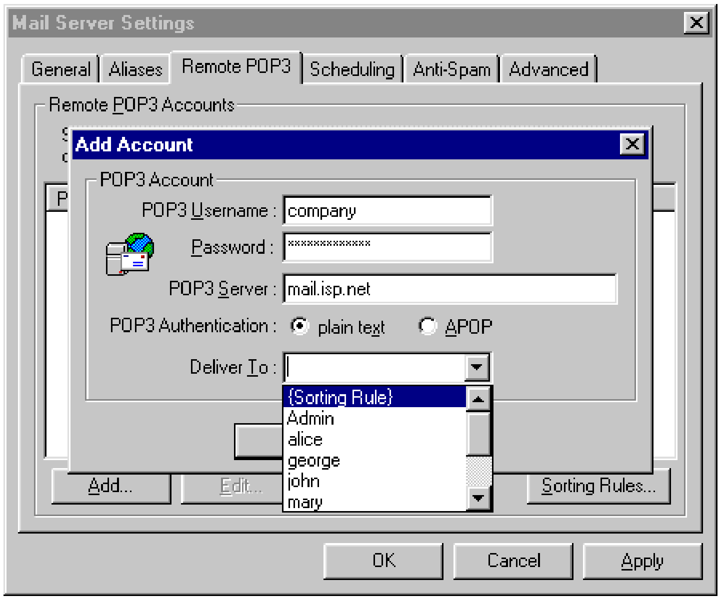


Exemplo

O seu provedor de acesso disponibilizou a caixa de correio company@mail.isp.net. Você pode ter o domínio company.com mas todo o e-mail para o seu domínio (sales@domain.com, john@domain.com) vai para a caixa de correio company@mail.isp.net no provedor de acesso.

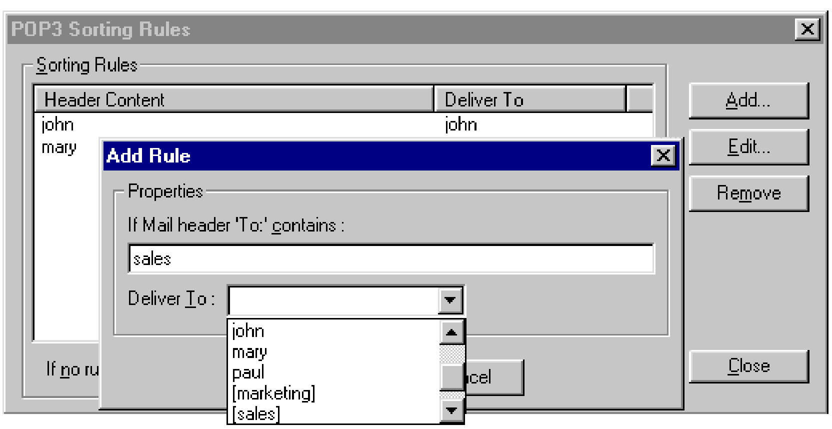
1 Vá ao menu *Configurações=>Servidor de correio=>POP3 remoto*, adicione uma nova conta e insira os seus detalhes

2 No campo "Entregar para:" selecione "Regras de classificação"



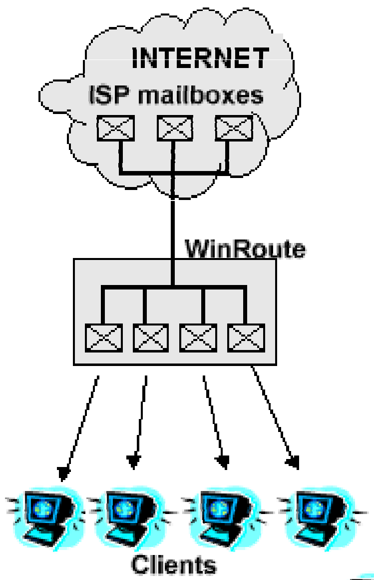
3 Pressione o botão Regras de classificação e adicione novos critérios. O WinRoute entregará o e-mail baseado no endereço de e-mail do destinatário, emitente ou assunto

4 Na mesma caixa de diálogo selecione um usuário ou grupo de usuários para os quais o e-mail pode ser entregue.



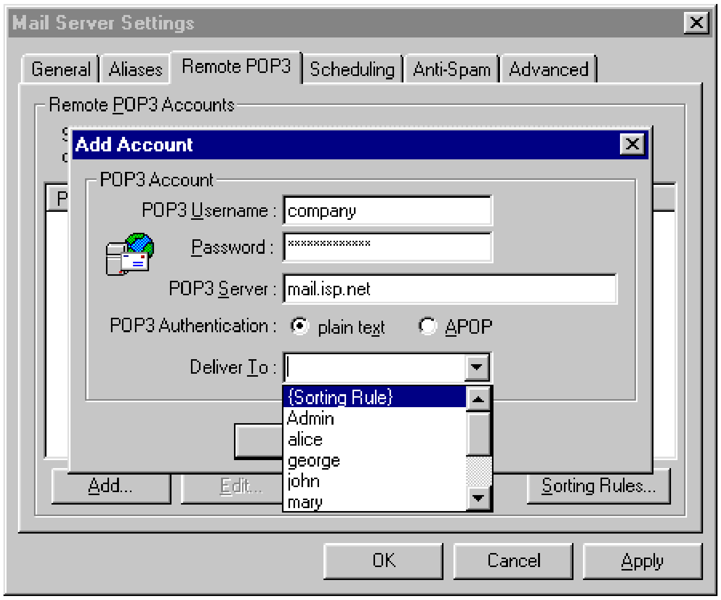
Recebendo e-mail - você tem diversas caixas de correio no provedor de acesso

O WinRoute pode verificar diversas contas em vários provedores de acesso e distribuir automaticamente as mensagens recebidas para as caixas de correio dor destinatários.



1 Vá ao menu *Configurações=>Servidor de correio=>POP3 remoto*, adicione uma nova conta e insira os seus detalhes.

2 No campo "Entregar para:" selecione o destinatário ou o grupo de destinatários



Configurações do software cliente de e-mail

Nesta seção

Usando o servidor de correio do WinRoute

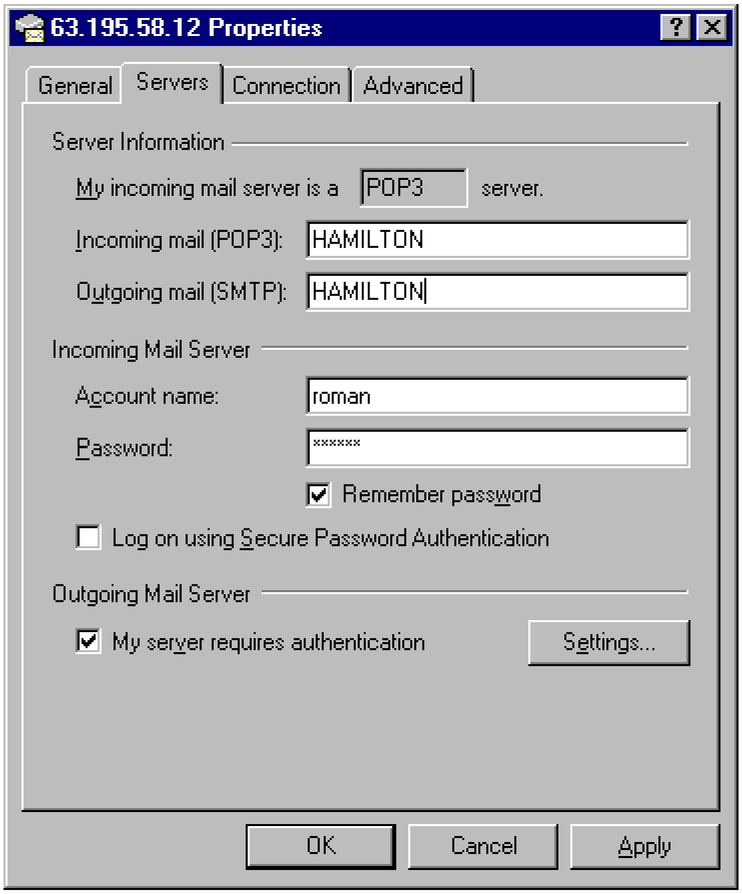
E-mail através do servidor de correio do WinRoute

Para fazer uso do servidor de correio do WinRoute você precisa configurar o seu **software cliente de e-mail**. O computador do WinRoute agirá como o servidor de correio de **entrada** e **saída**. Com resultado, você precisa informar o nome do computador do WinRoute no campo correto em seu software de e-mail. Se você tiver problemas no envio e recebimento de mensagens, recomendamos informar o endereço IP no lugar do nome do computador antes de passar a investigações posteriores. Algumas vezes o problema é com a resolução DNS em sua rede local, isto pode mostrar-se como você não estivesse usando o servidor DNS do WinRoute.

Exemplo:

O servidor de correio do WinRoute está executando em um computador com um endereço IP público atribuído dinamicamente e um endereço IP privativo igual a 192.168.1.1. O nome do computador é Hamilton (consulte a item Rede no Painel de controle).

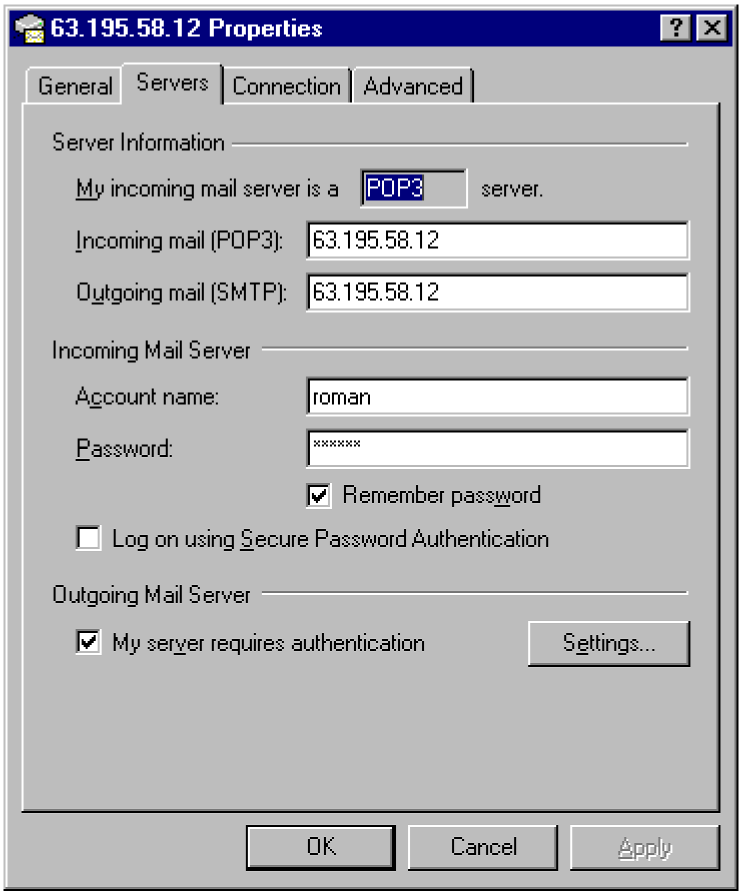
Você pode usar HAMILTON ou 192.168.1.1 nos campos de servidor de correio de Entrada (POP3) e Saída (SMTP) de seu software de e-mail.


63.195.58.12 Properties
General
Servers
Connection
Advanced
Server Information
My incoming mail server is a
POP3
server.
Incoming mail (POP3):
HAMILTON
Outgoing mail (SMTP):
HAMILTON
Incoming Mail Server
Account name:
roman
Password:
******
Remember password
Log on using Secure Password Authentication
Outgoing Mail Server
My server requires authentication
Settings...
OK
Cancel
Apply

Ignorando o servidor de correio do WinRoute

Você pode querer contornar o servidor de correio do WinRoute e receber ou enviar e-mail diretamente de um cliente de e-mail para o servidor de correio do seu provedor de acesso.

Se for o caso, informe o nome correto dos servidores de correio do seu provedor de acesso na configuração do servidor de correio de entrada e saída.



➢ ***Observação! Não configure o seu software cliente de e-mail para usar o proxy! Você precisa usar o NAT do WinRoute para o acesso à Internet e configurar o seu software***

cliente par ter acesso direto à Internet. Sua incapacidade em estabelecer uma troca de mensagens significa que o NAT não está configurado corretamente. Consulte a Lista de verificação ***para configurá-lo corretamente!***

CAPÍTULO 3

EXEMPLOS DE IMPLANTAÇÃO

Neste capítulo

Soluções com IPSEC, NOVELL e PPTP VPN

Nesta seção

IPSEC VPN

O WinRoute Pro 4.1 suporta IPSEC no assim chamado "**modo túnel (tunnel mode)**". O "**modo túnel**" pode suportar qualquer cliente IPSEC que permitirá que o endereço IP de transporte seja alterado.

Observação: O WinRoute não suporta software cliente do Checkpoint Secure Remote VPN.

Configurações do WinRoute:

Crie porta mapeada para ESP:

Protocolo: diferente de 50

IP de escuta: <não especificado>

IP de destino: o endereço de IP privativo do PC cliente

Sugerimos também a criação de uma porta mapeada para IKE. Isto não é necessário nos casos em que a comunicação é iniciada POR TRÁS do WinRoute para a Internet, contudo certas implementações do IPSEC podem exigir esta configuração:

Mapeamento de porta para IKE:

Protocolo: UDP

IP de escuta: <não especificado>

Porta de escuta: 500

IP de destino: o endereço IP privativo do PC cliente

Porta de destino: 500

Executando múltiplas sessões IPSEC simultaneamente

Podem haver mais clientes IPSEC para cada um dos quais você precise usar um endereço IP separado. Observação - o NAT do WinRoute permitirá que passem simultaneamente por ele tantos clientes você queira enquanto a conexão for iniciada A PARTIR da rede local e cada cliente esteja "usando" um endereço IP atribuído à interface externa do WinRoute.

Informações gerais sobre o IPSEC

O IPSec é um protocolo de criptografia de segurança usado para a comunicação segura entre dois computadores.

O IPSec usa o AH (Authentification Header) ou o ESP (Encapsulating Security Payload). O AH verifica apenas a identidade do remetente e o conteúdo do pacote. Os dados não são criptografados.

O ESP criptografa os dados. O ESP permite o uso do assim chamado "modo túnel" que é similar ao protocolo PPTP. O pacote então inclui o cabeçalho IP (necessário para transporte) que não está criptografado e a porção de dados que inclui o conjunto do pacote original criptografado.

O protocolo IKE (chamado algumas vezes de ISAKMP) é usado para a autenticação (troca de chaves de segurança). O IKE funciona sobre o protocolo UDP, porta 500. Esta porta é usada como origem e destino.

O AH usa o protocolo 51, o ESP usa o protocolo 50. O IPSec pode comunicar-se também com a autoridade certificadora inteira usando outros protocolos que não interferem com o NAT.

Nós incorporaremos o protocolo 50 dentro do WinRoute automaticamente de forma que não será necessário qualquer mapeamento de porta. A única condição para estabelecer a conexão automaticamente seria o início da mesma A PARTIR da rede local.

A maioria dos fornecedores de IPSec usa algoritmos MD5 e SHA1 para a autenticação e DES, 3DES e Blowfish para a criptografia. O IPSec não está estritamente vinculado a qualquer algoritmo específico de forma que soluções de fornecedores diferentes podem ser incompatíveis.

Novell Border Manager VPN

Usando o WinRoute Pro com o Novell BorderManager VPN (IPSEC)

Este documento descreve a configuração que torna possível conectar uma rede local que usa o NAT para compartilhar um único endereço IP fornecido pelo provedor de acesso a uma rede remota que usa a conectividade do Novell BorderManager Enterprise Server for VPN.

De acordo com o arquivo README.TXT fornecido no disquete de instalação do Novell BorderManager VPN Client,

"Você não pode usar o NAT no caminho entre um cliente VPN e um servidor VPN. Isto se deve ao fato de quando os pacotes IP e IPX são encapsulados e criptografados no cliente VPN, o endereço IP de origem que é usado para o encapsulamento é o endereço do cliente VPN. O cálculo do AH (Authentication Header) do IPSEC do pacote é baseado em seu endereço e o endereço de destino do servidor VPN. Então, se o endereço (do cliente VPN ou do servidor VPN) é modificado pelo NAT, o cálculo falhará quando o pacote chegar ao servidor VPN de destino e esse pacote será descartado. Mais provavelmente, entretanto, o NAT derrubará os pacotes do IPSEC porque apenas manipula pacotes do TCP, UDP e Internet Control Message Protocol (ICMP).

Quando você tem estações em uma intranet que precisa ter uma comunicação segura com redes protegidas por um servidor VPN através da Internet, sugerimos que use o Novell BorderManager Enterprise Edition site-to-site VPN (no lugar do client-to-site VPN)."

De qualquer modo, o Novell BorderManager Enterprise Server é muito caro para o usuário doméstico. Adicionalmente, ele exige uma configuração abrangente das rotas estáticas na rede remota à qual o acesso está sendo realizado. A solução sugerida acima pela Novell é então impraticável para as pessoas que gastariam de conectar sua rede local que usa NAT a uma rede remota via o Novell BorderManager VPN.

De forma espantosa, é possível conectar a rede local que usa o NAT a uma rede remota usando o WinRoute Pro e o Novell BorderManager VPN Client. Esta configuração permite a qualquer computador na rede local a ter acesso aos recursos na rede remota quando o túnel da VPN estiver estabelecido no computador do roteador. Nenhuma configuração é necessária na rede remota.

Abaixo estão os passos da configuração para a rede local.

Passo 1: Instale e configure o Novell BorderManager VPN Client no computador que será usado como um roteador. Certifique-se que a conexão da VPN à rede remota pode ser estabelecida com êxito e que não problema com o acesso aos recursos na rede remota.

Passo 2: Instale o WinRoute Pro no computador do roteador. Siga as instruções encontradas no Guia do Administrador referentes à configuração do WinRoute Pro e à configuração dos computadores na rede local para operar com o WinRoute Pro. Usa a configuração regular para o compartilhamento de um único endereço IP. Certifique-se que qualquer computador na rede local tem acesso aos recursos na Internet.

Passo 3: Quando você precisa do acesso aos recursos na rede remota, execute o Novell BorderManager VPN client no computador do roteador e conecte-se (faça o login) à rede remota.

Isto se torna possível pela arquitetura do WinRoute Pro. Em função dele funcionar no nível do IPSEC, a tradução/conversão de endereços ocorre antes do pacote ser roteado para o adaptador da rede virtual. Dessa forma os pacotes enviados ao servidor VPN têm o endereço IP de origem verdadeiro. No caminho de volta os pacotes recebidos do adaptador da rede virtual passam pela camada de tradução de endereço e são roteados para o computador certo n rede local.

As limitações desta configuração são que o login na VPN precisa ser feito manualmente no computador do roteador e que a conexão da VPN será encerrada após um certo período de inatividade que é definido no servidor VPN. Além disso, os pacotes IPX não serão roteados mesmo se o túnel da VPN tenha o protocolo IPX habilitado. Então, o encapsulamento do IPX estará disponível apenas no computador do roteador.

Acima de tudo, esta configuração é um meio econômico e conveniente de conectar uma rede local que usa o NAT a uma rede remota que usa o Novell BorderManager VPN.

Executando um servidor PPTP por trás do NAT

Para fazer funcionar um servidor PPTP na rede por trás do WinRoute (incluindo o computador no qual o WinRoute está sendo executado) você tem que configurar o mapeamento de porta.

> *Importante: Se o servidor VPN estiver na máquina host do WinRoute, você precisa mapear o endereço IP de destino para o* **endereço público***, não o privativo. O IP de escuta pode permanecer não especificado.*

Para o conexão de controle:

- Protocolo: TCP
- IP de escuta:
- Porta de escuta: 1723

- IP de destino: endereço IP de seu servidor PPTP (p.ex.192.168.1.12)
- Porta de destino: 1723

Para os pacotes GRE (PPTP):

- Protocolo: PPTP
- IP de escuta:
- IP de destino: endereço IP de seu servidor PPTP (e.g.192.168.1.12)

Após configurar o mapeamento de porta como mostrado acima você estará apto a colocar o seu servidor PPTP em qualquer lugar atrás do WinRoute INCLUINDO o computador COM o WinRoute. Os usuários terão acesso ao seu servidor PPTP ao "discar" para o endereço IP externo (público) de sua rede. Quando os pacotes chegarem ao computador do WinRoute serão encaminhados automaticamente para o computador certo atrás do firewall.

Exemplo de solução com PPTP

O WinRoute permite uma maneira muito econômica de criar a sua própria WAN entre filiais conectadas à Internet. Supomos que os leitores deste documento tenham um conhecimento básico de rede e WindowsNT.

A criação de uma WAN como essa é possível em diversos passos simples:

1 Verifique o ambiente:

NT Server nas duas pontas (filiais)

WinRoute Pro instalado nas duas pontas (filiais)

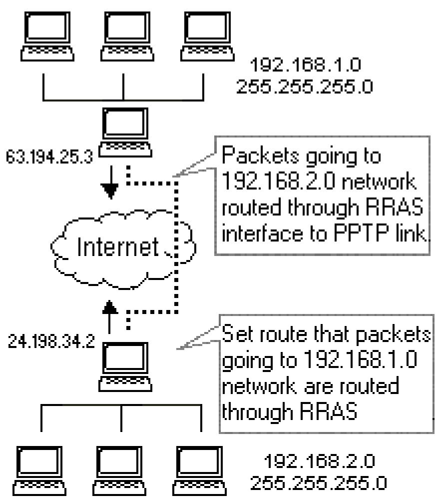
RRAS (Stealhead) instalado nos dois servidores NT

2 Crie uma rota estática em ambos os servidores NT especificando que os pacotes que vão para a outra rede (da outra filial) o farão através da interface do RRAS. Então - se você exibir as propriedades do TCP no log de depuração do administrador do WinRoute poderá ver uma interface de acesso discado listada entre as interfaces disponíveis .

3 Na administração do WinRoute, vá até a Tabela de interface e exiba as propriedades da interface AS usada para a conexão com o PPTP. Certifique-se que você não usará o NAT nessa interface.

4 Na guia RAS das propriedades da interface do RAS, selecione a conexão PPTP entre as entradas do RAS. Se você não estiver vendo a conexão pelo RAS entre as entradas, certifique-se de que escolheu o catálogo de telefones correto. Vá ao menu *Configurações->Avançadas->Opções variadas* e selecione o catálogo telefônico de RAS correto.

5 Teste a conexão - você deve estar apto a "pingar" a rede da outra filial e, ao mesmo tempo, ter acesso à Internet.



Executando clientes PPTP por trás do NAT

Não há a necessidade de configurações para o uso de clientes de PPTP por trás do WinRoute (NAT) com acesso ao servidor PPTP que está na Internet. Você pode estabelecer tantas conexões simultâneas quantas forem necessárias.

Solução com DNS

Nesta seção

Servidor DNS no PC do WinRoute

A execução de servidor DNS verdadeiro em um PC do WinRoute não trará quaisquer problemas. Todas as consultas ao DNS que chegam ao seu servidor (DNS) serão respondidas pelo endereço IP regular da Internet associado com aquele domínio. Um endereço IP como esse precisa estar associado com a interface de rede com conexão do PC do WinRoute à Internet e os servidores WWW escutam em ambas as interfaces pública e privativa.

Se o PC local envia uma consulta ao DNS para resolver o www.mydomain.com, ele recebe um endereço IP público associado com este domínio e conecta o servidor da Web com um endereço IP (que está atribuído à interface da Internet).

- ***Certifique-se que o mapeamento de porta para as consultas ao DNS está definido mesmo que você execute o servidor DNS no PC do WinRoute! Mapeie o protocolo UDP e a porta 53 para o endereço IP da interface da Internet.***

Servidor DNS por trás do PC do WinRoute

Você pode executar um servidor DNS verdadeiro em qualquer PC dentro de sua rede local. Para tanto você precisará configurar o mapeamento de porta:

Protocolo: UDP

IP de escuta: não especificado ou o endereço IP associado com o servidor DNS (mapeado como segundo endereço IP)

Porta de escuta: 53

IP de destino: o endereço de IP privativo da PC com o servidor DNS

Porta de destino: 53

Servidor DNS e WWW por trás do NAT

Se você executa os seus próprios servidores DNS e WWW na mesma rede privativa, pode querer abordar a seguinte questão:

Como eu administro as consultas ao DNS para www.mydomain.com vindas de minha rede local, como elas serão respondidas pelo endereço IP de rede privativa do servidor da Web enquanto as consultas ao DNS vindas da Internet receberão um endereço IP regular da Internet associado com www.mydomain.com?

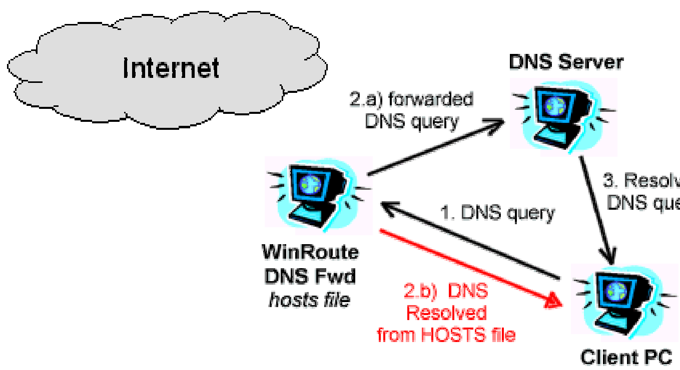
A solução é bastante simples e você usará o **forwarder DNS** embutido no WinRoute para resolver o problema. Em todos os PCs clientes você definirá o forwarder DNS do WinRoute como o servidor DNS. No PC do WinRoute você terá que efetuar as seguintes configurações:

- Ative o forwarder DNS do WinRoute
- Edite o arquivo HOSTS:

  No arquivo HOSTS, adicione um registro informando que www.mydomain.com está em um endereço IP privativo específico (aquele no qual o seu servidor da Web executa - p.ex. 10.10.10.8). O arquivo HOSTS é encontrado no diretório raiz do windows (onde o windows está instalado - c:\Windows ou c:\win98, etc.). Você também pode ter acesso ao arquivo HOSTS a partir da caixa de diálogo do forwarder DNS do WinRoute ao clicar no botão "Editar arquivo HOSTS".

Como irá funcionar?

Todas as consultas ao DNS enviadas pelos computadores clientes de sua rede local serão resolvidas primeiro pelo forwarder DNS do WinRoute. Todas as consultas serão comparadas primeiramente com os registros no arquivo HOSTS. Se o registro correspondente resolve a consulta, esta será respondida pelos detalhes em tais registros (endereço IP privativo no seu caso).



Se não houver qualquer registro no arquivo HOSTS que corresponda à consulta, essa será confrontada com os registros no cache do DNS do WinRoute (que está incluído no forwarder DNS do WinRoute). Se o cache do DNS não contiver registros que correspondam à consulta, essa será enviada ao servidor DNS que está definido no forwarder DNS do WinRoute para o encaminhamento de consultas.

Todas as consultas ao DNS vindas da Internet serão encaminhadas, com base nas configurações de mapeamento de porta, diretamente ao servidor DNS e resolvidas com base em seus registros.

- ***Observação! Em tal quadro você não pode executar o servidor DNS no mesmo computador do WinRoute. Isto se deve ao fato de que os dois serviços - forwarder DNS do WinRoute e o seu servidor DNS atuariam na mesma porta - UDP 53. Isto causaria um problema fatal.***

Questão com o DNS

Executando um servidor da Web (ou FTP, etc.) e servidor DNS na mesma rede privativa por trás do NAT do WinRoute

Você pode querer executar um servidor da Web com o domínio www.mydomain.com por trás do NAT e usar o seu servidor DNS, instalado na mesma rede, para a resolução de nomes.

Executando um servidor da Web (ou FTP, etc.) no PC do WinRoute.

Se você executa um servidor da Web no PC do WinRoute não terá quaisquer problemas com consultas locais. Todas as consultas ao DNS para www.whatever.com vindas ao seus servidor DNS serão respondidas pelo endereço IP regular da Internet associado com este domínio. Do mesmo modo um endereço IP precisa estar associado com a interface de rede conectando o PC do WinRoute à Internet e os servidores WWW podem escutar em ambas as interfaces pública e privativa.

Se o PC local envia uma consulta ao DNS para resolver www.whatever.com recebe um endereço IP público associado com este domínio. Como resultado isto conecta o servidor da Web com o endereço IP (que está atribuído à interface da Internet como descrito acima).

Executando um servidor da Web (ou FTP, etc.) em um PC por trás do WinRoute

Você pode querer executar um servidor da Web em um PC por trás do WinRoute (com um endereço IP privativo, p.ex. 10.10.10.8). O servidor da Web com domínio www.mydomain.com está fisicamente no endereço IP privativo 10.10.10.8 mas a sua consulta ao DNS será resolvida som um endereço IP regular (como 206.86.181.25) que está associado com este domínio.

Então o seu navegador ou cliente FTP irá dirigir-se ao endereço público, onde não existe qualquer servidor sendo executado como o servidor da Web que está dentro de sua rede.

Solução

Para resolver esta questão você precisa usar o **forwarder DNS** embutido no WinRoute como o servidor DNS dos seus computadores.

No arquivos **HOSTS** você irá adicionar uma outra entrada onde dirá que **www.mydomain.com** está funcionando no endereço IP **interno** (classe privativa) apropriado. Você deixará que o forwarder DNS olhe em seu arquivo HOSTS antes de enviar uma consulta DNS ao servidor regular.

Portanto, toda vez que os usuários enviam uma solicitação para **www.mydomain.com**, essas solicitações serão respondidas pelo endereço local apropriado.

Servidores WWW, FTP, DNS e Telnet por trás do WinRoute

Nesta seção

Executando o servidor WWW por trás do NAT

Para executar um servidor da Web por trás do NAT:

1. Vá ao menu *Configurações ->Avançadas ->Mapeamento de porta*
2. Adicione um novo mapeamento de porta:

   Protocolo: TCP

   IP de escuta: não especificado ou o endereço IP associado com o domínio. Do mesmo modo um endereço IP precisa estar associado com a interface

   Porta de escuta: 80

   IP de destino: informe o endereço IP do servidor da WEB (p.ex.192.168.1.10)

   Porta de destino: 80

Os usuários com acesso a estes serviços o farão com o uso do nome de domínio ou endereço IP público de sua rede. Após os pacotes chegarem ao WinRoute serão automaticamente desviados para o computador interno com o endereço IP interno apropriado.

Executando o servidor DNS por trás do NAT

O forwarder DNS embutido no WinRoute permite a você o encaminhamento de consultas ao DNS para um servidor DNS regular, para resolução de nome de domínio. Ele é capaz de resolver consultas locais ao DNS (ao usar o nome do computador local). De qualquer modo as consultas ao DNS tais como *www.whatever.com* precisam ser resolvidas pelo servidor DNS regular. O **forwarder DNS** do WinRoute **encaminhará** as consultas ao DNS para o **servidor DNS**.

Executando o servidor DNS por trás do NAT (WinRoute)

Para executar o servidor DNS por trás do NAT/WinRoute você tem que definir o mapeamento de porta como descrito abaixo. Os servidores DNS se comunicam entre si através do protocolo **UDP** na **porta 53**. Se você não efetuar esta configuração o seu servidor DNS não funcionará. Você precisa efetuar esta configuração. Ao executar o servidor DNS no mesmo computador do WinRoute, o módulo de inspeção do WinRoute executa o NAT **ANTES** que os pacotes cheguem a qualquer aplicação, incluindo o servidor DNS.

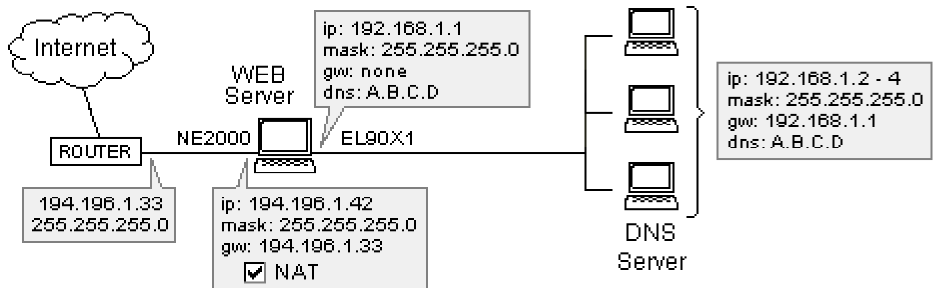
Protocolo: UDP

IP de escuta: não especificado ou endereço IP público do servidor DNS com o qual você quer operar

Porta de escuta: 53

IP de destino: endereço IP público ou privativo de servidor de nome de domínio (DNS)

Porta de destino: 53



➢ ***Observação!*** *Não é possível* ***executar um servidor DNS regular no mesmo computador do forwarder DNS do WinRoute. Ambos os serviços usam o protocolo UDP na porta 53. A execução de ambos os serviços DNS no mesmo PC causaria problemas fatais no roteamento de IP. Contudo, você pode desligar o forwarder do WinRoute se quiser executar o servidor DNS no PC do WinRoute.***

Executando o servidor FTP por trás do NAT

Para executar um servidor FTP por trás do NAT:

1. Vá ao menu *Configurações ->Avançadas ->Mapeamento de porta*
2. Adicione um novo **mapeamento de porta**:

Protocolo: TCP

IP de escuta: não especificado ou endereço IP associado com o domínio. Tal endereço IP precisa estar associado com a interface da Internet

Posta de escuta: 21

IP de destino: informe o endereço IP do servidor FTP (p.ex.192.168.1.10)

Porta de destino: 21

Executando um servidor FTP com uma porta diferente da padrão:

Ajuste o mapeamento de porta para corresponder à porta usada pelo servidor FTP.

Executando o servidor de correio por trás do NAT

Para executar um servidor de correio por trás do WinRoute recomenda-se que você crie duas entradas no mapeamento de porta - uma para o protocolo SMTP (que opera na porta 25) e uma para o protocolo POP3 (que opera na porta 110). Isto permitirá que outros servidores SMTP cheguem ao seu servidor SMTP e também você estará apto a receber e-mail pelo POP3 da Internet.

É necessário configurar o mapeamento de porta no caso do servidor de correio estar executando no computador do WinRoute. Isto se deve à posição do módulo de inspeção WinRoute que opera abaixo da pilha TCP de forma que os pacotes são alterados/recusados antes de chegarem ao sistema operacional.

Protocolo SMTP:

Protocolo: TCP

IP de escuta:

Porta de escuta: 25

IP de destino: informe o endereço IP do servidor de correio SMTP (p.ex.192.168.1.10)

Porta de destino: 25

Protocolo POP3:

Protocolo: TCP

IP de escuta:

Porta de escuta: 110

IP de destino: informe o endereço IP do servidor de correio POP3 (p.ex.192.168.1.10)

Porta de destino: 110

Executando o servidor Telnet por trás do NAT

O Telnet é amplamente empregado por muitas empresas para operar dados remotamente. Em especial, os servidores AS400 usam este protocolo.

Para executar um servidor Telnet por trás do WinRoute é necessário configurar o mapeamento de porta para o protocolo TCP na porta 23. Não são necessárias configurações para a execução do cliente Telnet com acesso ao servidor Telnet na Internet.

Protocolo: TCP

IP de escuta: não especificado ou endereço IP do servidor Telnet

Porta de escuta: 23

IP de destino: informe o endereço IP do servidor Telnet (p.ex.192.168.1.10)

Porta de destino: 23

Questões com FTP usando portas fora do padrão

Nesta seção

Acesso ao servidor FTP com portas fora do padrão

Se você está atrás do WinRoute e quer ter acesso a um servidor FTP com um número de porta diferente de 21, você não receberá uma listagem de diretório. Para fazer isto funcionar você precisa fazer o seguinte:

1. Vá à máquina do WinRoute
2. Desligue o WinRoute Engine
3. Vá ao menu Iniciar->Executar na área de trabalho
4. Digite regedit para ter acesso ao Editor de registro;
5. Encontre a chave HKEY_LOCAL_MACHINE/SOFTWARE/TinySoftware/WinRoute/Module/0
6. Modifique o SpecParams de forma que o valor fique igual ao número da porta do servidor FTP ao qual você quer ter acesso
7. Ligue o WinRoute Engine novamente.

Isto pode permitir a qualquer um por trás do WinRoute a ter acesso a um servidor FTP na Internet com uma porta diferente do padrão.

- ***Observação! Você pode especificar múltiplas portas ao colocar um espaço entre cada um dos valores.***

Servidor FTP por trás do WinRoute usando uma porta fora do padrão

Em algumas circunstâncias (por exemplo um cliente corporativo por trás de um firewall) um usuário pode ter seu acesso a FTP restrito apenas ao modo **passivo**. Se um servidor FTP por trás do WinRoute está usando uma porta diferente do padrão, nenhum acesso no modo **passivo** consegue ser estabelecido. Isto se deve ao fato do WinRoute (por default) considerar a porta 21 para FTP, de forma que se o usuário deseja usar uma porta diferente, o WinRoute precisa ser ajustado. O procedimento a seguir corrigirá este problema e permitirá o acesso no modo **passivo**.

1. Vá à máquina do WinRoute
2. Desligue o WinRoute Engine
3. Vá ao menu Iniciar->Executar na área de trabalho
4. Digite regedit para ter acesso ao Editor de registro;
5. Encontre a chave HKEY_LOCAL_MACHINE/SOFTWARE/TinySoftware/WinRoute/Mport. Você poderá ver subpastas lá que incluem informações correspondentes aos mapeamentos de porta. Se não houver qualquer subpasta, não existe mapeamento algum.
6. Encontre a pasta com o mapeamento de porta baseado na porta usada pelo servidor FTP
7. Modifique a chave *"flags"* para ‘1’
8. Modifique a chave *"NatApp"* para ‘FTP’
9. Ligue o WinRoute Engine novamente.

Estas configurações "dirão" ao WinRoute que os pacotes vindos na porta que você definiu serão do protocolo FTP e, portanto, o WinRoute se responsabilizará pelos passos adicionais em termos da passagem deste protocolo complexo por ele.

Redes especiais

Nesta seção

Redes Token Ring

Conectando redes Token Ring

Token Ring é tipo de rede muito específico. Por isso, assumimos que apenas profissionais de rede tratam com Token Ring e não nos aprofundaremos em explicações detalhadas aqui.

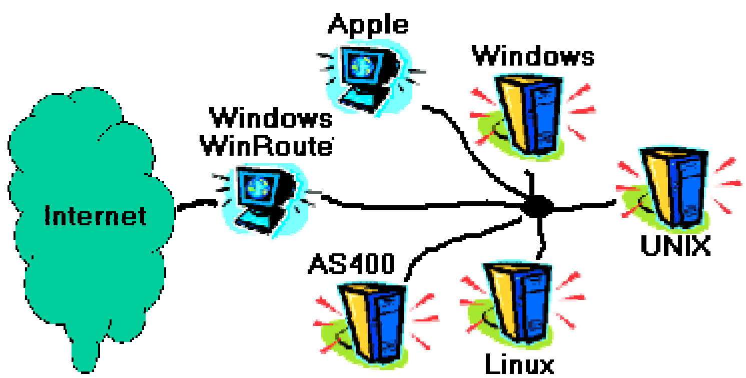
- Todos os computadores dentro da rede Token Ring precisam que o MTU (maximum transmission unit) seja ajustado para 1500
- No computador do WinRoute vá ao menu Configurações->Avançadas->Opções variadas e marque a opção "Suporte a redes Token Ring"
- Acompanhe outras instruções específicas de configuração para cada tipo de conexão à Internet

Ambientes com diversos sistemas operacionais (Linux, AS400, Apple)

Conectando ambientes com diversos sistemas operacionais (Linux, Unix, AS400, Apple)

O WinRoute é adequado para a conexão de ambientes com diversos sistemas operacionais à Internet. O WinRoute atua como um roteador de software. Como tal, ele suporta qualquer ambiente TCP/IP padrão.

➢ ***OBSERVAÇÃO: Um sistema operacional baseado no Windows precisa hospedar a aplicação WinRoute. Portanto, no mínimo um computador baseado em Windows 95/98/NT é necessário na rede do WinRoute. O host não pode de um sistema UNIX. Contudo, o UNIX pode operar como um sistema cliente.***



Conectando redes múltiplas

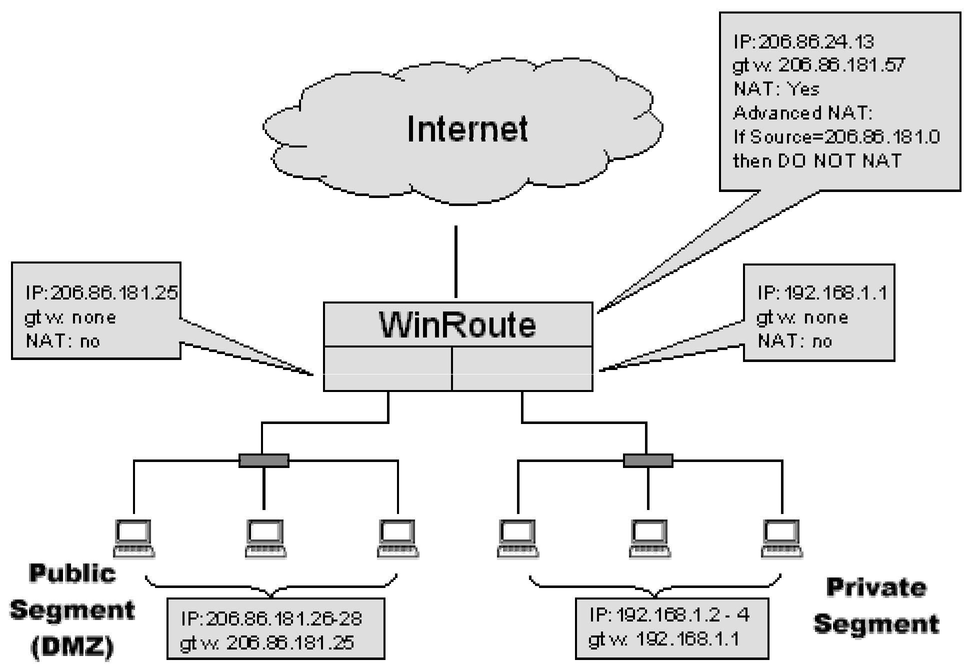
Nesta seção

Conectando segmentos públicos e privativos (DMZ)

Um segmento privativo consiste de computadores que usam endereços Internet do tipo privativo. Tais endereços são dedicados a redes privativas e não podem ser usados na Internet. Aí está porque você precisa do WinRoute para traduzir/converter estes endereços privativos em públicos o que deixa uma maneira de você conectar-se à Internet. Os computadores com endereços privativos não estão diretamente acessíveis de fora da própria rede (Internet).

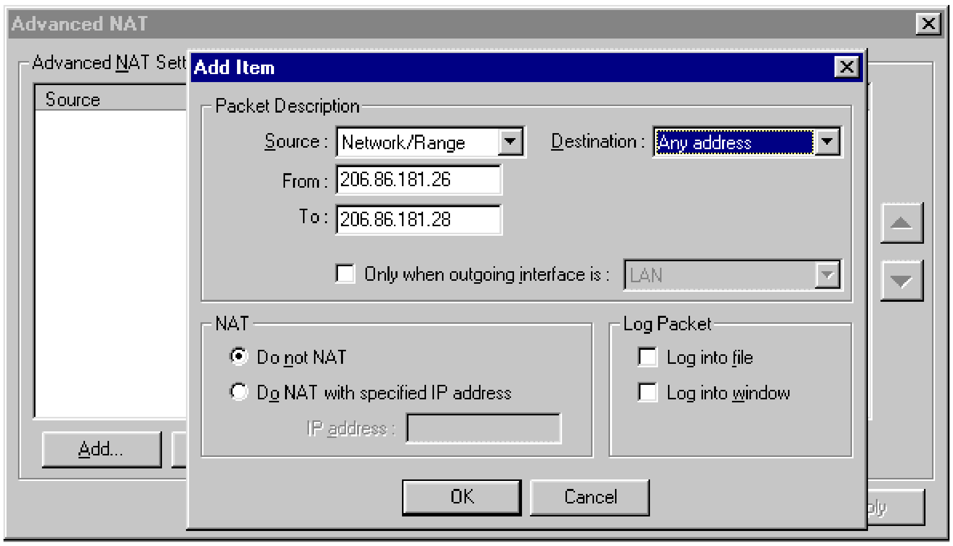
Um segmento público consiste de computadores onde cada um deles tem um endereço IP público. Estes sistemas, se as suas regras de segurança permitem, podem estar diretamente acessíveis pela Internet

Cada segmento tem que ter sua própria interface de rede no computador do WinRoute. Então o WinRoute Engine permite aos seus segmentos público e privativo o compartilhamento de uma conexão à Internet.



Configurações do WinRoute

Não é necessário efetuar configurações avançadas do NAT de forma que o WinRoute não executará o NAT para pacotes que saem do segmento público. Para isto vá ao menu Configurações=>Avançadas=>NAT.



Configurações de redes públicas e privativas

Estas redes serão configuradas da mesma maneira descrita em outras partes do manual. Para segmentos públicos a única diferença é que você usará endereços IP públicos nos mesmos. Basicamente mantenha as seguintes regras:

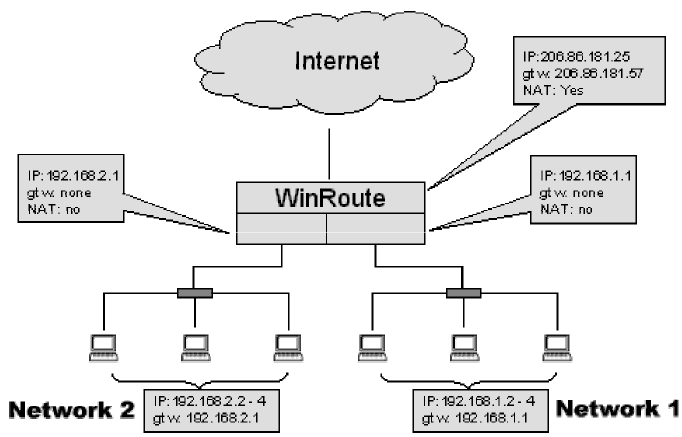
- SEM gateway default nas interfaces do WinRoute
- O endereço IP destas interfaces será usado como gateway default para o resto de sua rede.
- SEM NAT nas interfaces do WinRoute

…consulte a ***Lista de verificação*** para explicações adicionais

Compartilhando a conexão para duas redes com 1 endereço IP

No case de você ter duas redes conectadas à Internet através de um computador com o WinRoute, não são necessárias configurações específicas. Basicamente existem diversos segmentos dirigidos ao computador do WinRoute, onde cada um tem uma interface de rede separada. Em nosso exemplo existem três interfaces de rede no computador do WinRoute:

- Interface com a Internet
- Interface com a rede 1
- Interface com a rede 2



As únicas configurações necessárias que devem ser lembradas são:

Interface com a Internet

NAT está habilitado
Endereço IP definido de acordo com o seu provedor de acesso
Gateway definido de acordo com o seu provedor de acesso

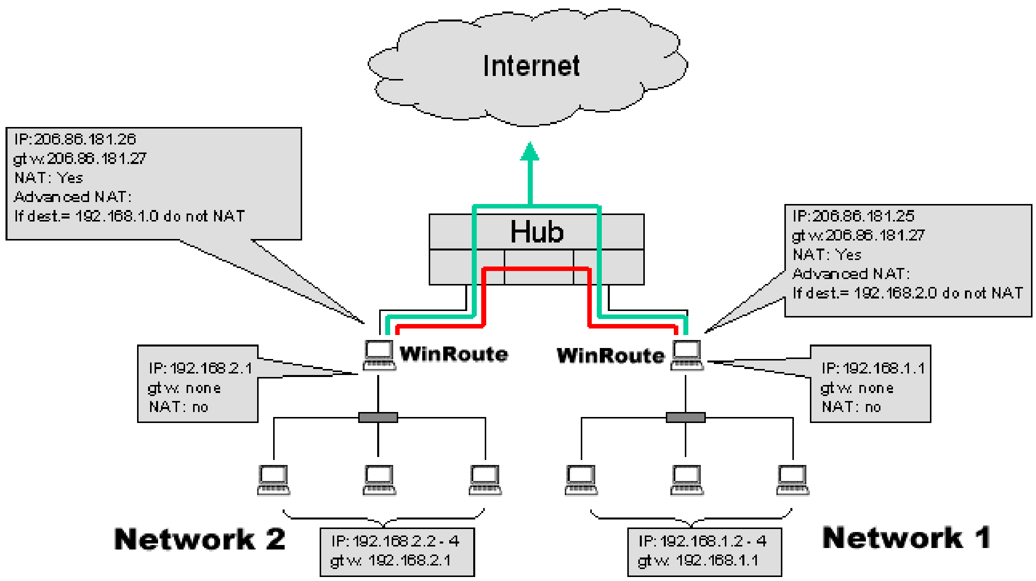
Interfaces internas

NAT NÃO está habilitado
NÃO há gateway default definido em ambas as interfaces
Endereço IP definido como do tipo interno (p.ex.192.168.1.1)

As outras configurações são as mesmas já descritas em outras seções deste manual. O tráfego que chega de cada sub-rede é roteado para a outra sub-rede ou para a Internet e vice-versa.

Compartilhando a conexão para duas redes com 2 endereços IP

Você quer compartilhar um acesso à Internet entre duas redes quando cada uma está por trás de um endereço IP público separado. Ao mesmo tempo você pode querer o acesso aos computadores em ambas as redes privativas.



Então é MUITO importante, quando da execução do seguinte quadro de roteamento, que:

- NÃO USAR O NAT com todos os pacotes que vão para a outra rede.
- USAR O NAT com todos os pacotes que vão para a Internet

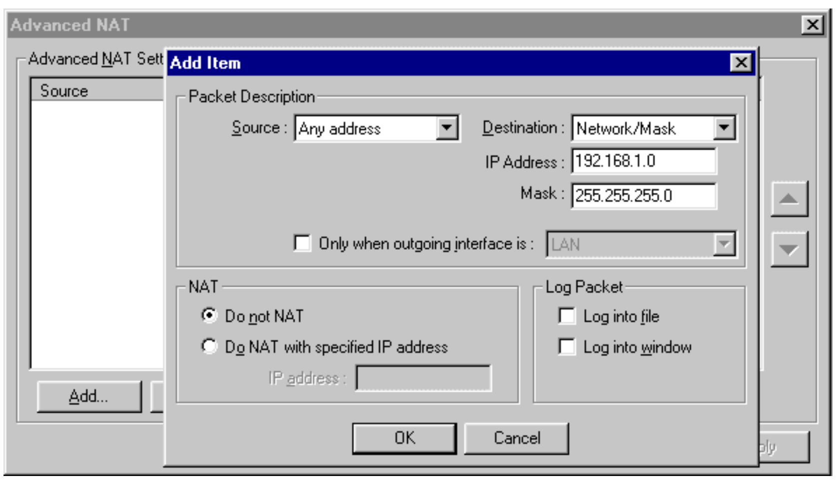
Em outras palavras, o WinRoute executará o NAT baseado no destino dos pacotes IP de passagem. Os pacotes que vão para a rede remota não serão modificados enquanto os pacotes que vão para a Internet serão alterados pelo NAT.

Roteador ou hub?

Com base em suas necessidades você precisa decidir se quer ou não usar um roteador entre as suas redes ou se um hub seria suficiente. Em nosso quadro há um hub fornecendo a funcionalidade necessária para permitir a duas redes o compartilhamento de uma conexão (de alta velocidade) à Internet.

Para configurar o WinRoute de forma a não executar o NAT com base no destino do pacote:

1. Vá ao menu Configurações->Avançadas->NAT.
2. Insira o critério de destino - normalmente a sub-rede ou uma faixa de endereços IP
3. Selecione a opção "Não usar o NAT"



Dica: Na configuração avançada do NAT você encontrará outra opção de não usar o NAT com base no endereço IP de origem. Esta configuração pode ser útil quando você sabe quais estações não precisam ter acesso à Internet. Então, ao invés de definir o critério do firewall você pode encontrar outra solução nas configurações avançadas do NAT.

Se você não usar o NAT com pacotes específicos, isto é, a origem permanece como o endereço IP interno, eles nunca receberão respostas. Em outras palavras, tal usuário pode tentar conectar-se à Internet para sempre sem nunca ter a chance de um acesso à ela (Internet).

Remote Access Server (discagem e acesso à Internet)

Solução do servidor de acesso remoto (RAS)

De vez em quando é necessário que você tenha acesso à sua rede corporativa do mundo externo via telefone e com o uso do acesso à Internet. O WinRoute fornece esta funcionalidade no WindowsNT com serviços RAS instalados e configurados.

Existem regras específicas que precisam ser aplicadas:

- Sua rede corporativa tem uma sub-rede (p.ex. 192.168.1.0)
- O servidor DHCP do WindowsNT está dando, aos usuários vindos através do RAS, endereços IP de uma sub-rede diferente (p.ex. 192.168.2.0)
- O NAT será executado apenas na interface de conexão à Internet

Em outras palavras, a placa de rede (NIC) ligada à sua rede local precisa ter o endereço IP de uma sub-rede (p.ex. 192.168.1.1) enquanto o usuário que se conecta ao seu servidor RAS precisa obter um endereço IP de uma rede diferente (p.ex. 192.168.2.1). O WinRoute atua como o roteador - ele pode rotear pacotes entre duas ou mais interfaces de redes diferentes - não da mesma.

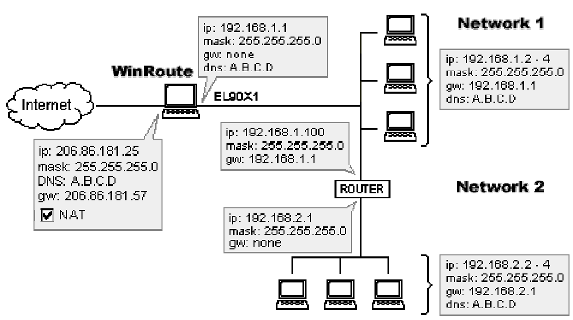
Este tipo de configuração parece-se com um pequeno provedor de acesso. O WinRoute não limita o número de usuários com acesso simultâneo ao seu servidor NT. Uma vez que o seu servidor NT fornece a usuários remotos endereços IP de sub-redes diferentes (outra que não a rede principal), o que limita o quantidade de usuários é o número de interfaces do RAS instaladas.

Conectando segmentos em cascata através de 1 endereço IP

A configuração da rede, onde todas as redes que estão para ser conectadas não se dirigem diretamente ao computador do WinRoute, enquanto são conectadas através de um roteador é chamada de rede com segmentos em cascata.

Figure 1: Connecting cascaded segments to the Internet

O roteador entre as duas redes pode ser qualquer um roteador baseado em hardware, computador com WindowsNT ou com qualquer Windows 95/98 e com o WinRoute. O WinRoute atuará como um roteador executando ou não o NAT.



Em geral é necessário "dizer" ao computador do WinRoute para onde os pacotes de entrada para outras redes serão enviados enquanto, para os pacotes de saída, precisa haver um conexão similar no roteador (dividindo as duas redes) especificando para onde os pacotes de saída da segunda rede serão enviados. Isto pode ser feito através da adição de novas rotas - uma no computador do WinRoute (para os pacotes de entrada) e uma no roteador (para os pacotes de saída).

- A ROTA nos computadores do WinRoute (membro da rede 1) irá rotear os pacotes IP da outra rede (rede 2) para o endereço IP específico da rede 1 no roteador. Este roteador irá transmitir posteriormente estes pacotes.
- A ROTA DEFAULT no roteador (conectando duas redes) irá rotear todos os pacotes que vêm da rede 2 para o endereço IP da rede 1 no computador do WinRoute. Em seguida o WinRoute irá tratar destes pacotes com o NAT e enviá-los para a Internet.

Exemplo

Nosso exemplo tem duas redes: 192.168.1.x e 192.168.2.x.. O roteador está em 192.168.1.100.

Observação! Como roteador você pode usar qualquer modelo baseado em hardware mas também qualquer computador com Win95/98 ou WindowsNT e com o WinRoute.

Configurações da rede 1 (rede primária)

- Você tem que dizer ao computador de WinRoute: "Todos os pacotes que vão para a rede 192.168.2.0 têm que fazê-lo através do roteador 192.168.1.100":
- 1. Vá ao prompt do MS-DOS
- 2. Digite o seguinte comando:

```
Route -p add 192.168.2.0 mask 255.255.255.0
192.168.1.100
```

- No roteador 192.168.1.100, a rota default deve se dirigir ao computador com o WinRoute, isto é, 192.168.1.1. Em outras palavras, você precisa dizer ao seu roteador para rotear todos os pacotes que vão para a Internet através do PC do WinRoute.
- Todas as outras configurações da rede serão feitas como descrito em outros capítulos (Configurando a rede).

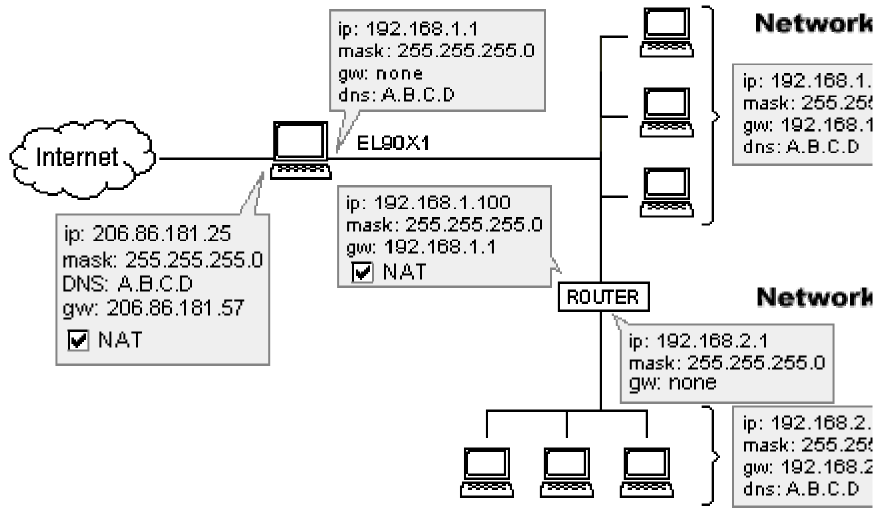
Configurações da rede 2 (rede secundária)

Todas configurações são regulares onde a rede 2 será a rede independente. O gateway default em todos os computadores da rede 2 será definido para o endereço IP da rede 2 no roteador (192.168.2.1 em nosso exemplo).

NAT entre a rede 1 e a rede 2

Você pode usar o WinRoute com o NAT "ligado" para conectar as redes primária e secundária. A rede secundária se mostrará como um único computador de forma que você se beneficiará de uma administração mais fácil e uma maior segurança na rede secundária. Você deve definir corretamente as configurações avançadas do NAT já que não deseja modificar o tráfego entre as duas redes.

Figure 2: Connecting cascaded segments to the Internet



Configurações avançadas do NAT no PC do WinRoute dividindo a rede 1 e a rede 2

Baseado no endereço IP de destino você poderá ou não executar o NAT. Em nosso exemplo, se o destino dos pacotes estiver na rede 192.168.1.0 então os pacotes não passarão pelo NAT. Isto permitirá a comunicação entre estas duas redes como se não o NAT não estivesse presente.

Para as configurações de rede siga as regras descritas no restante deste manual.

Adaptadores Ethernet multiporta

Das mais de 170,000 redes atualmente usando o WinRoute Pro como a sua solução de roteador/firewall, a configuração mais comum envolve duas placas de rede (NICs), uma para a Internet e a outra para uma rede local (LAN). Esta configuração básica filtra pacotes que vão e vem da Internet; contudo, ela não pode filtrar pacotes que trafegam entre segmentos locais porque eles não passam o tráfego através do WinRoute. Um exemplo desta configuração está ilustrado abaixo na figura 1.

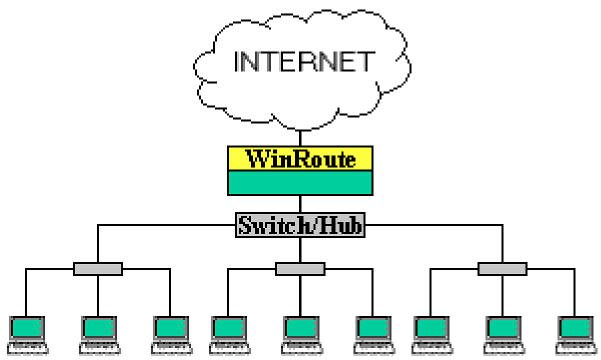


Figura 1. A configuração mais comum do WinRoute Pro.

Em muitos casos, uma terceira placa de rede será adicionada à máquina do WinRoute permitindo a existência de um segmento seguro em separado. Em tal quadro os pacotes que vem e vão ao segmento seguro a partir da Internet e de outros segmentos locais são filtrados pela WinRoute fornecendo um nível extra de segurança.

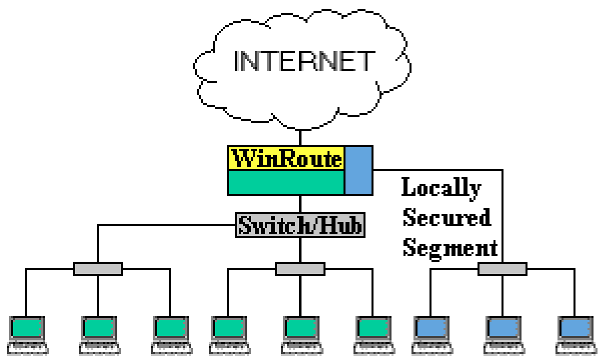


Figure 2. Um segmento separado para a rede local pode ser adicionado com o uso de uma terceira placa de rede.

Para redes maiores, que podem ter diversos segmentos separados com as suas próprias políticas únicas de segurança, o problema que vem a tona é que o número destes segmentos separados é limitado ao número de portas na máquina do WinRoute. Em função disto, é necessário hardware adicional para os corretos roteamento/comutação e políticas de segurança adicionais. Com a recente introdução das placas de rede Ethernet multiporta há a oportunidade do WinRoute de ser o único controlador do tráfego da rede. Uma vez que as placas multiporta podem permitir que a máquina do WinRoute passe a trabalhar com até 24 portas, dependendo do número de slots na placa mãe, a máquina do WinRoute pode também ser o servidor, o roteador, o switch, o controlador de domínio, etc. Dessa maneira a administração da rede pode ser centralizada e controlada através de um único ponto. A figura 3 ilustra o WinRoute Pro usando uma placa de rede Ethernet multiporta para controlar três redes separadas.

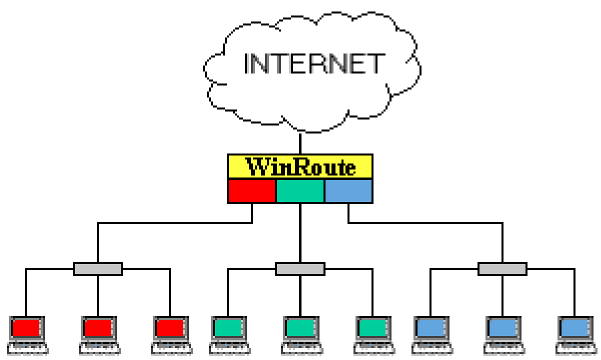


Figura 3. O WinRoute Pro equipado com uma placa de rede Ethernet multiporta.

Além da segurança melhorada e da administração centralizada possíveis com as placas de rede Ethernet multiporta, benefícios adicionais incluem balanceamento de carga e proteção contra falhas. Observe a atribuição de três portas ao segmento do meio na figura 4.

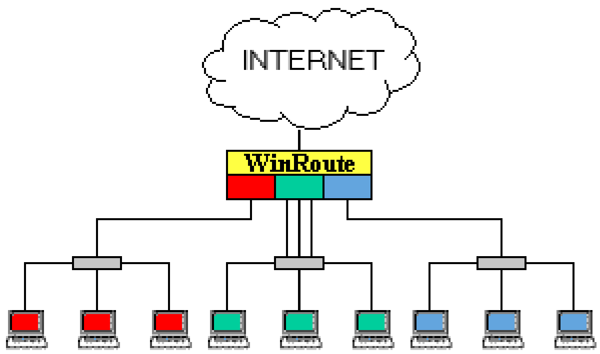


Figura 4. O segmento do meio tem três portas atribuídas para a agregação de portas.

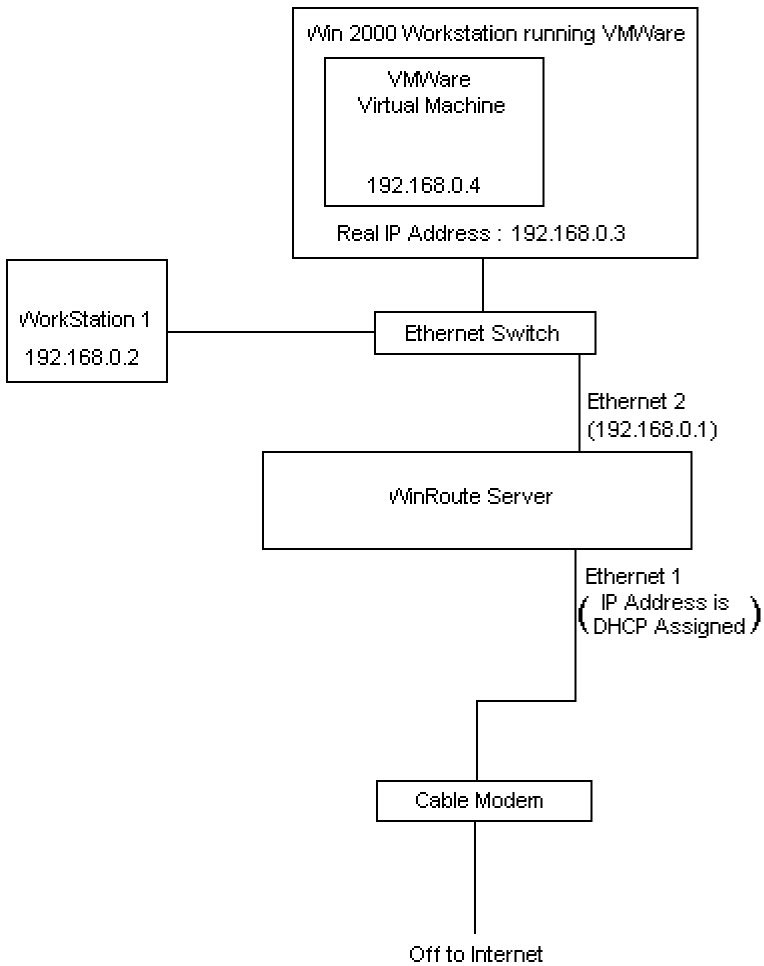
O balanceamento de carga pode ser obtido pela agregação de portas. Por exemplo, na figura acima o segmento no meio da rede está atribuído a três portas. Se este segmento usa um switch para conectar-se à máquina do WinRoute, cada um dos três computadores pode recuperar dados a 100 Mbps. Os outros dois segmentos apenas podem recuperar um total combinado de 100Mbps cada porque apenas uma porta daqueles segmentos está ligada à máquina do WinRoute. Um funcionalidade extra da agregação de portas é a proteção contra falhas na porta. Se uma linha fica sem conexão, o tráfego será roteado para a próxima porta disponível.

O uso das placas multiporta com o WinRoute pode fornecer um sistema de múltiplo roteamento efetivo, mas muito eficiente a um preço mais acessível e tudo sob um única cobertura administrativa. O WinRoute tem sido testado com êxito com as placas **D-Link 4 port DFE 570 TX** e **Adaptec 2 port Duralan ANA-62022**. Nenhuma outra placa foi testada.

Deve ser observado que este tipo de projeto de rede exige sub-redes diferentes para cada segmento de rede ligado à máquina do WinRoute.

VMWare

VMWare é uma aplicação que pode emular o PC em que está instalada até o nível do hardware. Para a rede, este computador virtual é visto como uma entidade completamente separada. Uma vez que o computador virtual tem as suas propriedades particulares de rede, o WinRoute contará a máquina virtual como um computador adicional.



CAPÍTULO 4

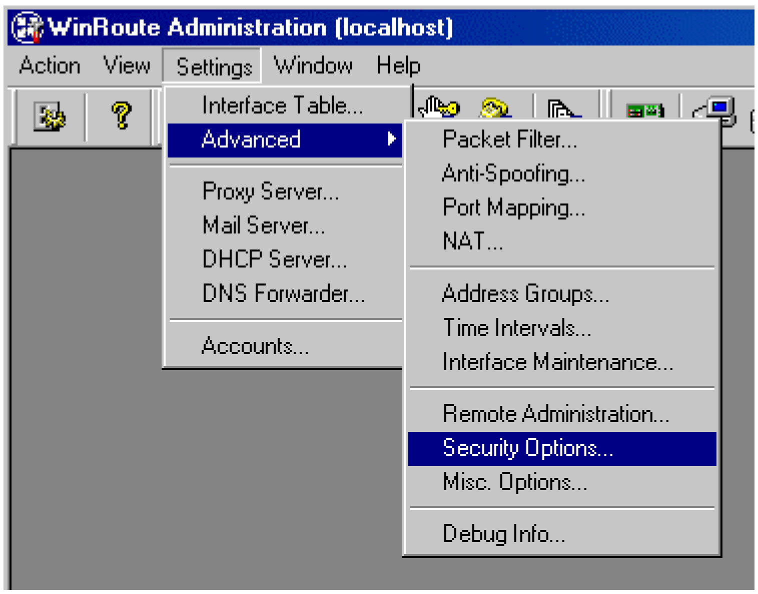
CONFIGURAÇÃO DO FIREWALL

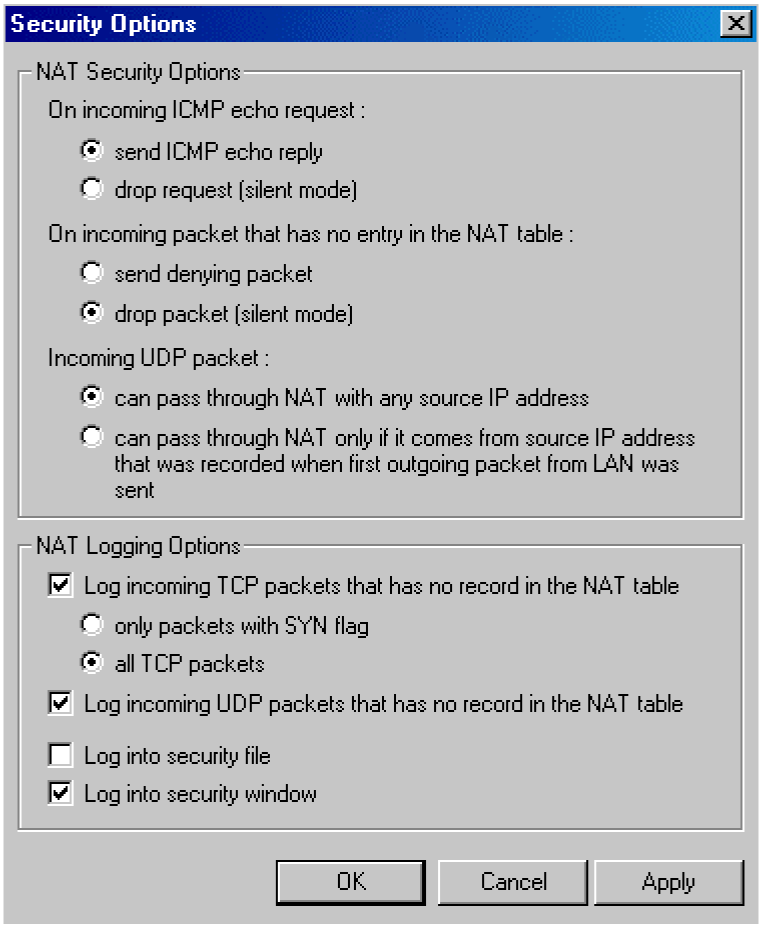
Neste capítulo

Encontre a alocação de porta correta

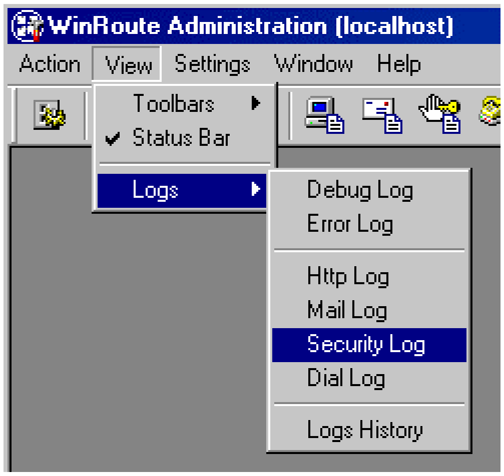
➢ ***Se você tiver o build 19 ou superior>***

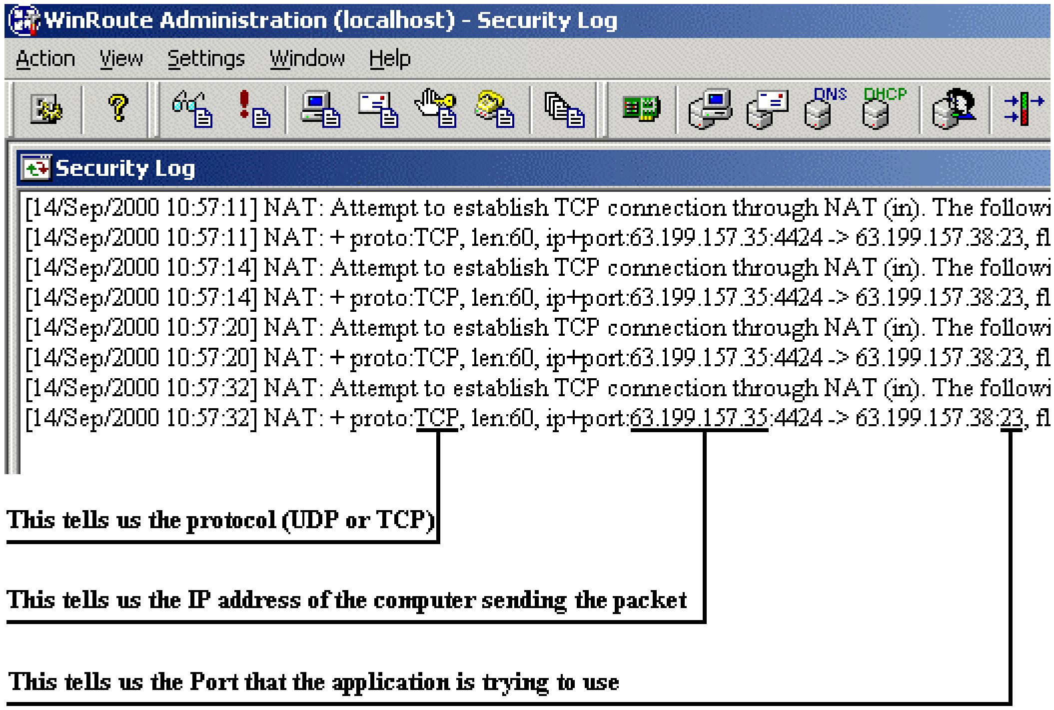
Na janela de Administração selecione Configurações-> Avançadas-> Opções de segurança




Security Options
NAT Security Options
On incoming ICMP echo request :
send ICMP echo reply
drop request (silent mode)
On incoming packet that has no entry in the NAT table :
send denying packet
drop packet (silent mode)
Incoming UDP packet :
can pass through NAT with any source IP address
can pass through NAT only if it comes from source IP address that was recorded when first outgoing packet from LAN was sent
NAT Logging Options
Log incoming TCP packets that has no record in the NAT table
only packets with SYN flag
all TCP packets
Log incoming UDP packets that has no record in the NAT table
Log into security file
Log into security window
OK
Cancel
Apply

Na parte inferior da janela de opções de segurança estão umas poucas opções de registro no log. Habilite, para a janela de segurança, o registro de log dos pacotes TCP e UDP que não são conhecidos pela tabela do NAT. Isto fará apenas o registro do log dos pacotes iniciados de fora do WinRoute. O WinRoute derrubará estes pacotes a menos que os mapeamentos de porta tenham sido feitos. Uma vez que esta é uma condição limitada de registro de log, apenas veremos um número selecionado de pacotes de maneira que será mais fácil encontrar a descrição do pacote que estamos procurando. O próximo passo é abrir a log de segurança a partir do menu Exibir-> Registros de log.





Neste caso, um computador em 63.199.157.35 envia um pacote da porta 4424 para a porta 23 no computador 63.199.157.38. A porta 23 é a porta padrão para telnet. Se você tinha uma servidor telnet executando em algum endereço privativo como 192.168.1.3 este poderia estar escutando a porta 23. Então você pode mapear os pacotes TCP na porta 23 para 192.168.1.3.

Serviços de troca de mensagens e telefonia

Existem atualmente diversos serviços de mensagem instantânea que suportam transferência de arquivo assim como chat de pc para pc (pc to pc chat) ou de pc para telefone (pc to phone chat). O WinRoute Pro tem sido testado com êxito com as seguintes configurações do **AOL instant messenger**, **Yahoo instant messenger**, **MSN Messenger**, e **ICQ**.

O **AIM** não exige quaisquer configurações específicas. Use as configurações default de conexão e certifique-se de não especificar que está usando um servidor proxy.

Os usuários do **Yahoo IM** precisam mudar as login preferences -> connection para "No network detection". Todos os serviços do Yahoo IM podem funcionar corretamente por trás do NAT com esta configuração.

O **MSN Messenger** funciona melhor com o uso do proxy HTTP. Habilite o proxy do WinRoute na porta default 3128 (além do Network Address Translation - NAT). O chat de PC para PC não funciona por trás do WinRoute; porém, o PC para telefone funciona.

O **ICQ** funciona na maioria dos casos com as configurações default da **última** versão. Se você tiver problemas na transferência de arquivos recomendamos o uso do proxy HTTP encontrado em preferences -> connections -> server and firewall. Habilite o proxy do WinRoute na porta default 3128 (além do Network Address Translation - NAT).

Observação: Você não precisa mapear quaisquer portas para qualquer uma destas aplicações.

H.323 - NetMeeting 3.0

O WinRoute inclui o suporte ao H.323. Isto significa que todas as aplicações de voz sobre IP podem se comunicar através do WinRoute. Tais aplicações são o Microsoft NetMeeting, CuSeeMee, telefonia pela Internet (você pode executar o Siemens IP phone através do WinRoute, por exemplo) e outros.

Se a comunicação é iniciada por trás do WinRoute

Em tal caso não são necessárias quaisquer configurações. O Winroute suportará virtualmente um número ilimitado de conexões simultâneas.

Se a comunicação é estabelecida da Internet para o PC por trás do WinRoute

Em tal caso é necessário criar o mapeamento de porta, em outras palavras para dizer ao Winroute para onde rotear os pacotes H.323 que chegam. Você precisa definir o seguinte mapeamento de porta:

Protocolo:	TCP
IP de escuta:	não especificado ou o endereço IP usado para comunicação com H.323 no caso de um sistema multihome
Porta de escuta:	1720
IP de destino:	O endereço IP da rede local da aplicação H.323
Porta de destino:	1720

O protocolo H.323 não está sendo executado apenas na porta 1720 - o WInRoute adicionará as outras conexões automaticamente. Em função da limitação do protocolo H.323 apenas uma estação pode usar tal comunicação de cada vez.

IRC - Internet Relay Chat

Não há a necessidade de configurações especiais para executar o cliente de IRC . Mesmo o DCC (Direct Chat/Send(Receive) Files) funcionará automaticamente se você usar a porta 6667 em seu IRC.

Para executar o servidor de IRC por trás do NAT mapeie as seguintes portas:

Protocolo: TCP

IP de escuta: não especificado ou o IP que você deseja usar para o servidor de IRC

Porta de escuta: 6667

IP de destino: endereço IP do PC com o seu servidor de IRC

Porta de destino: 6667

O uso de qualquer coisa que não a porta padrão fará com que o DCC não funcione.

CITRIX Metaframe

O WinRoute suporta totalmente o protocolo **CITRIX Metaframe**. Para ter acesso ao servidor do CITRIX Metaframe em execução dentro da rede do WinRoute a partir da Internet você tem que efetuar o seguinte mapeamento de porta:

Para o CITRIX Metaframe:

Protocolo: TCP

IP de escuta: não especificado ou o endereço IP público que você quer que o servidor use

Porta de escuta: 1494

IP de destino: endereço IP de classe privativa do servidor dentro da rede

Porta de destino: 1494

Você pode criar mais portas mapeadas e ter acesso a mais servidores simultaneamente. Para isso você precisa predefinir nos computadores clientes qual porta eles usarão para ter acesso ao servidor. Isto pode ser especificado no arquivo .ini do cliente - quando você cria o ícone da conexão.

MS Terminal Server

O WinRoute suporta totalmente o protocolo **MS Terminal Server**. Para ter acesso ao MS Terminal Server em execução dentro da rede do WinRoute a partir da Internet você tem que efetuar o seguinte mapeamento de porta:

Para o MS Terminal Server:

Protocolo: TCP

IP de escuta: não especificado ou o endereço IP público que você quer que o servidor use

Porta de escuta: 3389

IP de destino: endereço IP de classe privativa do servidor dentro da rede

Porta de destino: 3389

Você pode criar mais portas mapeadas e ter acesso a mais servidores simultaneamente. Para isso você precisa predefinir nos computadores clientes qual porta eles usarão para ter acesso ao servidor. Isto pode ser especificado no arquivo .ini do cliente - quando você cria o ícone da conexão.

Telefonia na Internet - BuddyPhone

O WinRoute é o primeiro software de roteador/firewall do setor que traz a telefonia na Internet para o sério nível dos negócios. O BuddyPhone permite que você faça uma ligação através da Internet a partir de uma rede para outra.

O suporte ao BuddyPhone funciona melhor com o ICQ. Registre este mensageiro instantâneo gratuito e você desfrutará de uma operação do tipo "um clique no botão" ao chamar seus amigos.

Todos os usuários ativos em sua lista ICQ buddy serão exibidos no seu catálogo telefônico do BuddyPhone e fazer uma ligação é tão fácil como selecionar um usuário na lista.

Não há necessidade de configurações n medida em que você use o BuddyPhone em conjunto com o ICQ.

Usando o BuddyPhone sem o ICQ

O WinRoute pode desviar as chamadas que vem da Internet para o destinatário certo na rede local com base na porta.

Use as portas 710 e acima para atribuir os usuários locais com as suas portas proprietárias.

Exemplo:

Você tem três usuários em sua rede local usando o BuddyPhone.

Nome do usuário	Endereço IP interno do usuário	Porta atribuída ao usuário
John	192.168.1.2	710

Quido	192.168.1.3	711
Bob	192.168.1.4	712

Então você definirá o mapeamento de porta:

Porta de escuta	IP de destino	Porta de destino
710	192.168.1.2	700
711	192.168.1.3	700
712	192.168.1.4	700

A realização da chamada telefônica para o usuário será tão fácil como digitar company.com:port# na caixa de diálogo de discagem direta (direct dial) do BuddyPhone. Por exemplo, sales.gamerouter.com:711.

- ***Observação! Não é erro na nossa documentação! A porta de destino é realmente 700. Este é o número de porta usado pelo BuddyPhone para trabalhar. O WinRoute fornecerá o roteamento baseado na porta de escuta.***

CU-SeeMe

O seguinte mapeamento de porta é necessário para recebimento de chamadas do **CU-SeeMe** através do NAT:

Protocolo: UDP

IP de escuta: <não especificado>

Porta de escuta: 7648

IP de destino: o endereço IP da estação que executa o cliente do CU-SeeMe

Porta de destino: 7648

Protocolo: UDP

IP de escuta: <não especificado>

Porta de escuta: 7649

IP de destino: o endereço IP da estação que executa o cliente do CU-SeeMe

Porta de destino: 7649

Limitações:

- No momento, não é possível executar mais de um cliente CU-SeeMe na rede local
- Não é possível conectar-se a um "refletor" protegido por uma senha.

Acesso remoto - PC Anywhere

Nesta seção

PC Anywhere

O WinRoute inclui o melhor suporte ao PC AnyWhere da Symantec do que qualquer software roteador do mercado. O PC AnyWhere permite ao usuário ter acesso a administrar computadores dentro da rede. Para fazer isto você tem que adotar o seguinte quadro:

1. O computador a ser administrado irá executar o PC Anywhere Host.
2. O computador remoto irá executar o PC Anywhere Remote
3. O mapeamento de porta no computador do WinRoute será configurado desta maneira:

   Protocolo: TCP/UDP

   IP de escuta: não especificado

   Porta de escuta (faixa): 5631-5632

   IP de destino: endereço IP do PC Anywhere Host dentro de sua rede (p.ex.192.168.1.12)

   Porta de destino: 5631-5632

Questão de segurança

Para aumentar a segurança e impedir a abertura de sua rede para o mundo exterior, o WinRoute permite aos usuários escolher um endereço IP específico a partir do qual o acesso é permitido através de portas específicas. Esta configuração permite apenas que certos computadores ou redes tenham acesso ao seu sistema pela Internet.

Para configurar os computadores que têm permissão de acesso à sua rede, você precisa definir primeiramente um grupo de endereços (mesmo que você informe apenas um único computador). Para configurar isto vá ao menu Configurações=>Avançadas=>Grupos de endereços.

Mudando o acesso a diferentes computadores

Você pode definir os direitos do administrador no WinRoute para habilitar uma conexão diretamente ao host do WinRoute. Enquanto estiver no host, você pode alterar o IP de destino no mapeamento de porta e ter acesso diretamente ao PC que escolher. Incrível!

PC Anywhere gateway

A execução do pcAnywhere em seu modo gateway no firewal do WinRoute permitirá ao cliente remoto encontrar uma lista dos hosts pcAnywhere disponíveis em execução por trás do firewall. A partir desta lista você pode administrar qualquer um dos hosts pcAnywhere por trás do firewall do WinRoute.

Estes passos presumem que você está usando o pcAnywhere 9.0 e não está filtrando quaisquer pacotes de entrada/saída no firewall do WinRoute

- Os computadores administrados por trás do firewall do WinRoute executarão o PC Anywhere Host usando TCP/IP
- O computador remoto executará o PC Anywhere Remote usando TCP/IP
- O pcAnywhere está instalado no firewall do WinRoute usando o modo Gateway. Ao configurar o dispositivo do gateway, ambos os dispositivos de entrada (Incoming) e saída (Outgoing) devem ser configurados para TCP/IP

- No firewall do WinRoute, o pcAnywhere precisa estar configurado para escutar na placa de rede interna (p.ex.192.168.1.1). Instruções sobre como configurar o pcAnywhere para escutar um endereço IP/placa de rede específico podem ser encontradas no site da Web da Symantec
- Adicione o(s) endereço(s) IP específico(s) do(s) computador(es) a ser(em) administrado(s) na opções de rede (network options) do pcAnywhere. Para fazer a varredura de toda a sub-rede use 255 como o último octeto (192.168.1.255).
- Configure o mapeamento de porta no WinRoute desta maneira:

  Protocolo: TCP/UDP

  IP de escuta: placa de rede externa (206.86.181.25)

  Porta de escuta: FAIXA (5631-5632)

  IP de destino: placa de rede interna (192.168.1.1)

  Porta de destino: 5631-5632

Seção de jogos

Nesta seção

Sobre a execução de jogos por trás do NAT

Usando jogos

Muitos jogos de hoje suportam um ambiente multiusuário. Os usuários podem lutar entre si pela Internet, rede local ou podem conectar-se a um dos servidores de jogos existentes na Internet. Os usuários também podem hospedar os seus próprios servidores de jogos e permitir a amigos, familiares ou pessoas totalmente estranhas a excitação de jogar em conjunto.

Existem muitos jogos que não exigem quaisquer configurações no WinRoute. Antes de tentar configurar o WinRoute para um jogo específico, recomendamos que você use o demo do jogo primeiro. Diferentemente dos servidores Proxy, a arquitetura básica do WinRoute suporta muitos jogos diretamente "da prateleira."

Certos jogos exigem a configuração de uma porta específica no WinRoute para serem ativados e funcionarem. As portas são usadas para uma identificação adicional do jogador no servidor do jogo (em geral).

Se o jogo tem uma porta específica associada com ele, isto não é um problema para o WinRoute! Apenas configure o mapeamento de porta do WinRoute para encaminhar os pacotes que chegam à sua rede para o computador do jogador por trás do firewall.

As portas usadas variam de jogo para jogo. Consulte a documentação que acompanha cada jogo ou ligue para o suporte técnico do fornecedor do jogo para mais informações. Este manual contém somente alguns exemplos das configurações para os jogos mais populares.

Aasheron's call

Asheron's call é um jogo popular na Microsoft Gaming Zone. Para jogar este jogo do computador por trás do GameRouter você tem que efetuar as seguintes configurações de mapeamento de porta:

1 Vá ao menu *Configurações->Avançadas->Mapeamento de porta*

2 Efetue as seguintes configurações:

Nome:	S1	S2	S3	S4
Número da porta:	2300-2400	9000-9013	6667	28800 - 29000
IP de destino:	IP do PC com o jogo	IP do PC com o jogo	IP do PC com o jogo	IP do PC com o jog
Protocolo:	TCP/UDP	UDP	TCP	TCP

Battle.net (Blizzard)

O seguinte mapeamento de porta deve ser definido para que você possa jogar partidas na battle.net. Apenas um usuário pode jogar de cada vez.

Protocolo: TCP/UDP

IP de escuta: não especificado

Porta de escuta: 6112

IP de destino: endereço IP do computador do jogador (p.ex.192.168.1.6)

Porta de destino: 6112

Half-Life

Half-Life

Protocolo: TCP/UDP

IP de escuta: não especificado

Porta de escuta: 27015

IP de destino: endereço IP do computador do jogador (p.ex.192.168.1.6)

Porta de destino: 27015

MSN Gaming zone

A configuração a seguir foi testada a fundo com MechWarior3 na **MSN Gaming Zone**. Apenas uma máquina pode ter acesso à MSN de cada vez.

1. Vá ao menu *Configurações->Mapeamento de porta*
2. Adicione um novo mapeamento de porta

   Protocolo: TCP

   IP de escuta: "não especificado"

   Porta de escuta: faixa de 2300 a 2400

   IP de destino: o endereço IP local da máquina na qual você quer se conectar à MSN

   Porta de destino: faixa de 2300 a 2400
3. Adicionar outro mapeamento de porta

   Protocolo: UDP

   IP de escuta: "não especificado"

   Porta de escuta: faixa de 28800 a 28912

IP de destino: o endereço IP local da máquina na qual você quer se conectar à MSN

Porta de destino: faixa de 28800 a 28912

Quake

Quake 3

Clientes do Quake 2/3

Não há necessidade de configurações especiais

servidor do Quake 2/3 Server

Para o servidor Master:

Protocolo: UDP

IP de escuta: não especificado

Porta de escuta: 8002 (single)

IP de destino: x.x.x.x

Porta de destino: 8002

Para clientes conectando-se ao servidor do Quake3 Arena:

Protocolo: UDP

IP de escuta: não especificado

Porta de escuta: 27960 (single)

IP de destino: x.x.x.x

Porta de destino: 27960

StarCraft

Jogando o StarCraft

O WinRoute Pro incluí suporte sem igual para todos os jogadores do StarCraft (Blizzard Entertainment). Múltiplos jogadores na rede conectada à Internet através do WinRoute Pro podem desfrutar do divertimento ao jogar com seu "inimigos" virtuais na Internet.

No momento, o suporte totalmente automático funciona apenas no caso em que todos os jogadores ligados ao jogo a partir de uma rede estejam em computadores por trás do WinRoute Pro e não na máquina host.

Para mais detalhes visite www.tinysoftware.com

Mapeamentos adicionais para jogos/aplicações comuns

Portas necessárias para diversas aplicações

Age of Empires II - 2 mapeamentos de porta necessários

Protocolo: TCP

IP de origem: não especificado

Porta de origem: 47624

IP de destino: endereço IP da máquina que está executando a aplicação

Porta de destino: 47624

Protocolo: TCP/UDP

IP de origem: não especificado

Porta de origem: faixa 2300 - 2400

IP de destino: endereço IP da máquina que está executando a aplicação

Porta de destino: faixa 2300 - 2400

Delta Force

Protocolo: TCP

IP de origem: não especificado

Porta de origem: faixa 3568 - 3569

IP de destino: endereço IP da máquina que está executando a aplicação

Porta de destino: faixa 3568 - 3569

Dial Pad

Protocolo: UDP

IP de origem: não especificado

Porta de origem: faixa 51200 - 51201

IP de destino: endereço IP da máquina que está executando a aplicação

Porta de destino: faixa 51200 - 51201

Gamespy

Registro

Protocolo: UDP

IP de origem: não especificado

Porta de origem: 25635

IP de destino: endereço IP da máquina que está executando a aplicação

Porta de destino: 25665

Para os games (para si mesmos)

Protocolo: UDP

IP de origem: não especificado

Porta de origem: faixa 25000 - 30000

IP de destino: endereço IP da máquina que está executando a aplicação

Porta de destino: faixa 25000 - 30000

Kali - 3 mapeamentos de porta necessários

Protocolo: UDP

IP de origem: não especificado

Porta de origem: 2213

IP de destino: endereço IP da máquina que está executando a aplicação

Porta de destino: 2213

Protocolo: UDP

IP de origem: não especificado

Porta de origem: 6666

IP de destino: endereço IP da máquina que está executando a aplicação

Porta de destino: 6666

Protocolo: UDP

IP de origem: não especificado

Porta de origem: 57

IP de destino: endereço IP da máquina que está executando a aplicação

Porta de destino: 57

Mplayer

Protocolo: TCP/UDP

IP de origem: não especificado

Porta de origem: 8000 - 9000

IP de destino: endereço IP da máquina que está executando a aplicação

Porta de destino: 8000 - 9000

PCanywhere versões 2.0 - 7.51 - 2 mapeamentos de porta necessários

Protocolo: TCP

IP de origem: não especificado

Porta de origem: 65301

IP de destino: endereço IP da máquina que está executando a aplicação

Porta de destino: 65301

Protocolo: UDP

IP de origem: não especificado

Porta de origem: 22

IP de destino: endereço IP da máquina que está executando a aplicação

Porta de destino: 22

Quicktime - 2 mapeamentos de porta necessários

Protocolo: TCP

IP de origem: não especificado

Porta de origem: 554

IP de destino: endereço IP da máquina que está executando a aplicação

Porta de destino: 554

Protocolo: UDP

IP de origem: não especificado

Porta de origem: faixa 6970 - 6999

IP de destino: endereço IP da máquina que está executando a aplicação

Porta de destino: faixa 6970 - 6999

RTSP

Protocolo: UDP

IP de origem: não especificado

Porta de origem: faixa 6970 - 7170

IP de destino: endereço IP da máquina que está executando a aplicação

Porta de destino: faixa 6970 - 7170

VNC

Protocolo: TCP

IP de origem: não especificado

Porta de origem: 59xx (dependendo do número exibido)

IP de destino: endereço IP da máquina que está executando a aplicação

Porta de destino: 59xx

Protocolo: TCP

IP de origem: não especificado

Porta de origem: 58xx

IP de destino: endereço IP da máquina que está executando a aplicação

Porta de destino: 58xx

Glossário de termos

A

ARP

O Address Resolution Protocol associa um endereço IP a um endereço de hardware ao pedir à máquina de envio uma informação adicional chamada de endereço MAC. O WinRoute usa o ARP apenas para fins de log de maneira a aumentar a segurança.

B

BOOTP

O Bootstrap Protocol que simplesmente se refere àqueles computadores dentro de uma rede local que estão definidos para aceitar um endereço IP dinamicamente de um servidor DHCP.

C

Cache

Refere-se ao local onde os dados são armazenados temporariamente. O WinRoute usa o cache para armazenamento temporário de páginas da Web para manter a largura da banda.

Caixas de correio no WinRoute

As caixas de correio são mantidas em um diretório separado de onde o WinRoute está instalado. Normalmente em c:/Program files/WinRoute/Mail.

Não são criadas caixas de correio após a instalação mesmo que usuários sejam criados. As caixas de correio são criadas fisicamente APÓS a chegada do primeiro e-mail para um usuário.

D

DHCP

O Dynamic Host Configuration Protocol é um protocolo de organização e simplificação da administração de endereços IP de máquinas locais. Em muitos casos (tais como com o WinRoute) um servidor DNS está embutido no servidor DHCP para maior simplificação. Ao especificar o endereço IP de um dispositivo de rede em particular, normalmente o dispositivo ligado à Internet, o DHCP usará os valores do DNS associado com aquele dispositivo.

DNS

O Domain Name System é um método de nomeação para o endereçamento IP. Por exemplo, www.tinysoftware.com é um nome de domínio e tem um endereço IP associado. Um servidor DNS faz a correspondência dos nomes de domínio com um endereço IP. Nós usamos o sistema de nome de domínio (DNS) porque é mais fácil lembrar de um nome de domínio do que uma seqüência de números.

E

Endereço IP

O endereço IP é um número único de 32 bits, que identifica o computador em uma rede IP. Um único endereço IP é atribuído a cada computador na Internet. Cada pacote de passagem pela Internet contém a informação, de qual endereço foi enviado (endereço IP de origem) e para qual endereço ele deve ser remetido (endereço IP de destino).

Endereço MAC

O endereço Media Access Control (MAC) é mais específico que o endereço IP e não pode ser modificado porque é característico de cada dispositivo de hardware de rede.

ETRN

O ETRN é um comando usado pelos servidores SMTP para negociar uma maior tempo, após o estabelecimento de uma conexão o servidor SMTP pode fazer uma consulta por correio SMTP.

O comando ETRN é sempre usado onde um servidor SMTP não está "online" 24 horas e o e-mail de tal servidor SMTP precisa ser armazenado temporariamente em outro servidor SMTP.

F

Firewall

Um módulo de filtragem localizado em uma máquina de gateway que examina todo o tráfego de entrada e saída para determinar se ele pode ser roteado para o seu destino. O WinRoute fornece um firewall abrangente por meio de: funcionalidade do NAT, a atribuição de regras para endereços IP específicos e a habilidade de registrar certas informações que vão em uma direção de forma que possam ser autorizadas no caminho de volta.

Flags (sinalizadores)

Sinalizadores (Flags) são a parte das informações estendidas do pacote. Eles guardam as informações adicionais sobre o pacote usadas pelos roteadores. Aqui está a lista dos sinalizadores exibidos pelo WinRoute:

SYNC - Synchronize (sincronização) - o pacote de estabelecimento de uma conexão TCP

ACK - Acknowledge (conhecimento) - reconhecimento sobre a troca de dados

RST - Reset (reinicializar) - solicitação de um restabelecimento da conexão

URG - Urgent - pacote urgente

PSH - Push (empurrar) - solicitação de remessa imediata do pacote para as camadas superiores

FIN - Finalize (finalizar) - finalizar a conexão

FTP

O File Transfer Protocol é uma protocolo de aplicação usado para transferir, atualizar, excluir, mover, renomear ou copiar dados através da Internet.

G

Gateway

O ponto de entrada de uma rede para outra. Um gateway é responsável pela distribuição correta dos dados que entram e saem de uma rede local. O WinRoute precisa estar instalado na máquina do gateway, também chamada como o computador host.

I

ICMP

O Internet Control Message Protocol usa datagramas para relatar erros na transmissão entre o host e o gateway.

Interface de rede

A interface de rede é um dispositivo que conecta o computador com outros computadores por meio de um meio de comunicação. Uma interface de rede pode ser uma placa Ethernet, modem, placa ISDN, etc. O computador envia e recebe pacotes por meio da interface de rede.

IPSEC

O Internet Protocol Security, em resumo, permite as redes privativas virtuais a usarem a autenticação e a criptografia do emissor. O WinRoute suporta as variantes do IPSEC da Novel e da Cisco.

L

LAN (rede local)

Uma rede local (Local Area Network, LAN) é um grupo de computadores interconectados com a habilidade de compartilhar recursos.

M

Mapeamento de porta

O mapeamento de porta (ou Port Address Translation - PAT) é o processo no qual os pacotes que chegam à interface são verificados quanto ao número de porta e endereço IP aos quais eles querem chegar. Com base nos números de portas um endereço IP encontra estes pacotes que são encaminhados para o endereço IP predefinido de classe privativa na rede local.

Máscara de rede

A máscara de rede é usada para agrupar endereços IP. Há um grupo de endereços atribuídos a cada segmento de rede. Por exemplo, a máscara 255.255.255.0 agrupa um conjunto de 254 endereços IP. Se tivermos, por exemplo, uma sub-rede 194.196.16.0 com máscara 255.255.255.0, o endereços que poderemos atribuir aos computadores na sub-rede serão de 194.196.16.1 até 194.196.16.254.

N

NAT

Com o NAT - Network Address Translator - você pode conectar-se à Internet por meio de um único endereço IP e os computadores dentro da rede usarão a Internet como se estivessem conectados a ela diretamente (certas limitações se aplicam).

A conexão de uma rede inteira com o uso de um único endereço IP é possível uma vez que o módulo do NAT reescreve o endereço de origem nos pacotes enviados, dos computadores na rede local, com o endereço do computador no qual o WinRoute está sendo executado.

O NAT diferencia-se significativamente de vários servidores proxy e gateways de nível de aplicação pois esses, em princípio, nunca estariam aptos a suportar tantos protocolos como o NAT.

P

Pacote

Um pacote é uma unidade básica de dados de comunicação usada na transmissão de dados de um computador para outro. Cada pacote contém um certo montante de dados. O tamanho máximo do pacote depende do meio de comunicação. Como um exemplo, em redes Ethernet o tamanho máximo é de 1500 bytes. Em cada camada, podemos dividir o conteúdo do pacote em duas partes: a parte do cabeçalho e a parte dos dados. O cabeçalho contém informações de controle da camada em particular, a parte dos dados contém dados que pertencem à camada superior. Informações mais detalhadas da estrutura do pacote podem ser obtidas na seção de filtragem de pacotes.

POP3

O protocolo **POP3** é usado principalmente por software cliente de e-mail para pegar as mensagens nas caixas de correio em um servidor de correio compatível com o POP3. O servidor de correio do WinRoute tem tal capacidade também, isto é, pode pegar as mensagens automaticamente em qualquer servidor de correio compatível com POP3 e posteriormente distribui-las para as caixas de correio dos destinatários locais.

O protocolo POP3 é um protocolo **TCP** que funciona na **porta 110**. Se você quiser ter acesso a este servidor de correio em execução por trás do WinRoute ou no computador onde o WinRoute está instalado (para pegar s suas mensagens DA Internet) você tem que efetuar o **mapeamento de porta** do protocolo TCP, porta 110 enviado para o endereço IP de **classe privativa** do PC em que o servidor de correio está sendo executado.

Porta

Uma porta é um número de 16 bits (a faixa permitida vai de 1 até 65535) usado por protocolos da camada de transporte - os protocolos TCP e UDP. As portas são usadas para endereçar aplicações (serviços) que são executadas em um computador. Se houvesse apenas um única aplicação de rede em execução no computador, não haveria a necessidade de números de portas e apenas o endereço IP seria suficiente para o endereçamento de serviços.

Contudo, diversas aplicações podem ser executadas ao mesmo tempo em um determinado computador e nós precisamos diferenciá-las. É para isto que os números de portas são usados. Desse modo, um número de porta pode ser visto como um endereço de uma aplicação dentro do computador.

PPTP

PPTP - Point To Point Tunnelling Protocol - é um protocolo de VPN (Virtual Private Network) usado pelo sistema operacional da Microsoft para criar a conexão criptografada entre dois computadores.

Protocolo

Define regras para a transmissão de dados.

Proxy

O proxy é um outro método de compartilhar o acesso à Internet. O proxy opera com os dados em um nível mais alto de protocolo de forma que o compartilhamento de acesso à Internet com servidores proxy nunca foi confiável e também exigiu um gateway especial de aplicação para cada protocolo de rede.

R

RAS

O Remote Access Service refere-se à habilidade de discar para um outro computador ou rede remotamente. No contexto do WinRoute, o RAS simplesmente refere-se à uma conexão discada.

Registros MX

Os registros MX contém as informações sobre outros servidores de correio na Internet. Com o uso dos registros MX você pode contornar o servidor de correio do seu provedor de acesso e enviar e-mail diretamente para o servidor de correio de destino.

A vantagem está no caso do servidor de correio do seu provedor de acesso *não estar confiável*. Por outro lado, o fato de que você tenta enviar e-mail *diretamente ao destino* pode ter impacto no período de tempo da entrega do e-mail. No caso do *servidor de correio de destino* estar inacessível o e-mail poderia permanecer *parado* na fila de correio de saída do seu servidor de correio do WinRoute.

S

SMTP

O **SMTP** (Simple Mail Transfer Protocol) é usado na comunicação direta entre servidores de correio (tal como o servidor de correio do WinRoute e o servidor de correio do seu provedor de acesso) e para o envio de mensagens a partir do seu software cliente de e-mail. O SMTP é um protocolo de "uma via" - isto é, as mensagens podem ser enviadas ou recebidas pelo servidor de correio mas não é possível recolher as mensagens em qualquer outro servidor de correio com o uso deste protocolo.

O protocolo SMTP é um protocolo TCP que opera na **porta 25**. Se você quiser ter acesso a este protocolo com servidor de correio em execução por trás no computador do WinRoute (para permitir a outro servidor de correio que envie as suas mensagens ou para usar este servidor de correio para as suas mensagens de saída se você está em sua rede local) você tem que efetuar um **mapeamento de porta** do protocolo TCP, porta 25 enviado para um endereço IP de **classe privativa** do PC em que o servidor de correio está sendo executado.

T

Tabela de roteamento

As tabelas de roteamento são conjuntos de regras geradas pelos sistemas operacionais da Microsoft com base nas definições feitas na configuração do protocolo TCP/IP. A tabela de roteamento é usada pelo WinRoute como o conjunto de regras para rotear os pacotes. Para ver a tabela de roteamento vá à janela do prompt do MS-DOS e digite o comando `route print`.

TCP/IP

O TCP/IP é um somatório de protocolos de rede usados para a comunicação entre computadores. Todos os protocolos são baseados em pacotes, isto é, todos os dados enviados através de um protocolo são divididos em pequenas partes e enviados através da rede. Os protocolos TCP/IP são: IP, TCP, UDP, ICMP e outros baseados no IP.

U

UDP

O UDP (User Datagram Protocol) usa um tipo especial de pacote chamado datagrama. Os datagramas não exigem resposta, eles são apenas de "mão única". Os datagramas são normalmente usados para streaming media porque uma ocasional perda de pacote não afetaria o produto final da transmissão.

V

VPN

A VPN (Virtual Private Network) envolve múltiplas redes locais com a habilidade de compartilhar recursos através da Internet ao criar um túnel direto que faz a criptografia e a decriptografia em ambas as extremidades. O WinRoute suporta o VPN através do PPTP.

INDEX

A

B

C

D

E

F

G

H

R

S

T

U

V